imanami
GroupID

User Manual for Delivery

imanami
Solutions for Directory Management

Published By Imanami Corporation
2301 Armstrong St. Suite 211
Livermore, CA 94551,
United States

Copyright 2011 by Imanami Corporation.

All rights reserved. No part of this document may be reproduced or transmitted in any form or by means without the written permission of Imanami Corporation. Imanami made every effort in the preparation of this document to ensure the accuracy of the information. However, the information contained in this document comes without warranty, either expressed or implied. Imanami is not liable for any damage, cost or alleged cost either directly or indirectly by this document.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Prepared By

Imanami Technical Communications Team

Document Information

Document Version: 6.10.8.4
First Edition Release Date: December 15, 2010
This Release: May 27, 2011

Supported GroupID Version: 6.0

Feedback and Support

For feedback on this document, please write to:
techcomm@imanami.com

For complaints or technical support, please contact:
support@imanami.com

About This Document

Pre-requisites

This document assumes that you have read the Installation Guide and have GroupID running on your machine.

This Document

This document provides comprehensive information about GroupID and its use. The document targets administrators and IT managers and is not intended for the end users.

GroupID Documentation Roadmap

Step1:

Installation Guide

Step 2:

User Manual (this document)

Step 3:

Self-Service Style Guide

Table of Contents

1. **About This Document** 5
   - Pre-requisites 5
   - This Document 5
   - GroupID Documentation Roadmap 5

2. **Part 1 - Introduction** 1
   - Chapter 1: Getting Familiar with GroupID 2
     - GroupID Overview 3
     - What's New in GroupID 6.0 5
     - Launching GroupID 6
     - Licensing GroupID 7
     - The User Interface 8
     - Creating a Service Account for Active Directory and Exchange 11
     - Connecting to a Domain 13
   - Chapter 2: Group Management Concepts 15
     - Group Lifecycle Management 16
     - Group Classification 16
     - Security Types 17
     - Group Types 17
     - Group Scope 18
     - Group Deletion 18

3. **Part 2 - Self-Service** 21
   - Chapter 3: Introduction 22
     - Self-Service - Overview 23
     - Features 23
     - Requirements for Self-Service 25
     - Self-Service User Interfaces 26
   - Chapter 4: Setting Up a New Portal 32
     - Create a new Portal 33
     - Duplicate a Portal 39
     - Setting Functionality Mode 40
   - Chapter 5: Portal Configuration 42
     - Directory Settings 43
     - Web Server Settings 44
     - Security Settings 45
     - Support and Logging Settings 47
     - Notification Settings 49
     - Advance Settings 50
   - Chapter 6: Workflows 57
     - Overview 58
     - Workflow Events 58
     - System Workflows 60
     - User-defined Workflow 61

Configuring Notification 65
Managing Workflow Requests 66
Chapter 7: Customizing the Portal 69
Add Photo to User Profile 70
Display Types 71
Customize Search Form 91
Customize Update Wizard 93
Customize My Properties 96
Navigation Bar 98
Bad Words List 102
Rename Active Directory attributes 103

4. **Part 3 - Automate** **105**
Chapter 8: Introduction 106
Automate - Overview 107
Getting familiar with the User Interface 108
Active Directory and Exchange Permissions for Automate 114
Upgrading from Quest ActiveGroups to Automate 114
Chapter 9: Managing Groups 118
Creating a new Group 119
Creating a new SmartGroup 123
Updating Groups 130
Scheduling Jobs 132
Automate Command-line Utility 136
Moving Groups 137
Manage Group Owners 138
Group Expiry 141
Deleting Groups 148
Deletion Settings 149
Recycle Bin 150
Group History 151
Group Management Service 153
Chapter 10: Memberships 156
Group Members 157
Nesting Groups 163
Membership Settings 165
Chapter 11: Exchange Settings 168
Exchange Settings tabs 169
Applying Size Limit to Incoming Messages 170
Restrict Recipients for the Group 170
Selecting Expansion Server 172
Hiding Group from Address Lists 172
Hiding Group Membership from Address Book 173
Setting Group to Send Out-of-Office Message 173
Setting Recipient for Non-Delivery Reports 173
Assigning Values to Custom Attributes of a Group 173
Chapter 12: Dynasties 175

Dynasties - Overview 176
Creating a Dynasty 176
Dynasty Options 185
Dynasty Settings 188
Chapter 13: The Query Designer 191
Launching the Query Designer 191
General Query Options 194
Password Expiry Options 195
Storage Options 197
Active Directory Options 198
Database Options 200
Include / Exclude Options 202

5. **Part 4 - Synchronize** **205**
Chapter 14: Introduction 206
Synchronize - Overview 207
Features 207
Getting Familiar with the User Interface 208
Chapter 15: Job Management 211
Creating a Job 212
Password Policy Validation 223
Previewing Jobs 224
Running Jobs 226
Synchronize Command-line Utility 227
Scheduling Jobs 229
Job Files 231
Logging Job Run Activities 232
Chapter 16: Transformations 234
Static Transformation 235
Join Transformation 235
Substring Transformation 236
Left Transformation 237
Script Transformation 238
Chapter 17: Scripting 240
The Script Editor 241
Scripting Environments 244
DTM Object 245
Getting Familiar with the Global Script Editor 252
VB Options Set by Synchronize 255
Scripting Restrictions by Synchronize 255
.Net Assembly References 255
.Net Namespaces 256
Chapter 18: Synchronize Options 257
Customizing the Job Run Chart 258
Setting the Columns to Display for a Job 258
Setting the Columns to Display for Jobs History View 258
Setting the History Threshold Value 258

Delimiters 259

6. **Part 5 - Reports 261**
Chapter 19: Introduction 262
Overview 263
Getting Familiar with the User Interface 263
Report Categories 263
Output Formats 266
Chapter 20: Working with Reports 267
Generate a New Build Criteria for Report 268
Report Files 275
Generate Report from Build Criteria 276
Reports Command-line Utility 276
Edit Report Build Criteria 278
Delete Build Criteria 279
Scheduling Reports 280

7. **Part 6: Password Center 285**
Chapter 21: Introduction 286
Password Center - Overview 287
Features 287
Requirements for Password Center 287
Password Center User Interfaces 288
Chapter 22: Setting Up a New Portal 291
Identity Stores 292
Creating a New Portal 304
Chapter 23: Portal Settings 310
General Settings 311
Identity Store Settings 311
IIS Settings 312
Security Settings 313
Support Settings 314
Miscellaneous Settings 315

8. **Part 7: GroupID Configurations 319**
Log Settings 320
Logging Configuration 321
Notifications Settings 323
Group Name Prefixes 324
Database and the Data Service Settings 325
Creating a new database 326
Connecting to an existing database 327
History Settings 327
Exchange Version Setting 329

9. **Index 331**

Part 1 - Introduction

This part of the user manual covers the fundamental concepts you need to know to use GroupID. To practice along while going through this part, you should have GroupID installed on your computer. To learn about installing, configuring and licensing GroupID, please refer to the GroupID Installation Guide.

Chapter 1: Getting Familiar with GroupID, familiarizes you with the GroupID Management Console.

Chapter 2: Group, introduces you to basic Group Management concepts.

Chapter 1: Getting Familiar with GroupID

This chapter provides an overview of GroupID and gets you familiarized with its user interface. You will also learn how to connect the GroupID snap-in to a domain. The chapter is divided into following sections:

GroupID Overview, provides general information about GroupID and its modules.

What's New in GroupID 6.0, describes the new features introduced in GroupID 6.0.

Launching GroupID, provides instructions on launching GroupID.

The User Interface, introduces you to GroupID Management Console's user interface.

Creating a Service Account for Active Directory, provides instructions on how to create a new service account and grant it permissions on Active Directory and Exchange objects.

Connecting to a Domain, provides instruction on how to connect GroupID to an Active Directory domain controller.

GroupID Overview

GroupID is a suite of applications that provides Group and Identity Management solutions for your enterprise needs. Built upon the foundation of Imanami's best selling products WebDir, SmartDL, SmartR and DTM, GroupID takes the concept of automation and flexible management one step further. GroupID extends the capabilities and features of these products with the next generation replacements by integrating all modules into a single unified user interface.

GroupID Automate offers enhanced administration and automation features for Active Directory groups. Use Automate to create and update group memberships dynamically when changes occur within your organization. Share your administrative responsibilities with others by assigning multiple owners to groups while you are out of office. Create Private, Semi-Private, Semi-Public and Public groups depending on the level of control and access you want to grant for group membership. Create groups with a limited life span, setting them to renew, expire and automatically be deleted from the source directory keeping your directory clean and preventing group glut.

A new addition to the GroupID suite, Password Center offers a new way for your administrators to save themselves from the mundane tasks of unlocking user accounts and resetting passwords. Use Password Center to create portals for your network users from where they can carry out these tasks on their own. Create separate portals with respect to domains, directory services, data sources, and departments in your organization; or with respect to any other formation according to your organizational needs. Customize, personalize, localize and secure each portal and make them available to your users through your corporate intranet or the Internet.

With Password Center, you can do more than just setup portals for password management. You can also extend your Active Directory password policy by applying more conditions that subject passwords to more complexity than that offered by Active Directory out-of-the-box.

GroupID Reports lets you analyze and monitor your Active Directory and Exchange server activities and collect statistical information about critical objects, thus enabling you to have an up-to-date picture of your directories and servers.

Reduce the overhead on your network administrators and empower your users to carryout common tasks, such as updating their own information within Active Directory. Assign responsibilities at various levels by authorizing specific users to manage Groups, Contacts or Users. Define Workflows to route user requests through assigned authorities for approval. Achieve all this and a lot more by creating Web portals with GroupID Self-Service.

GroupID Synchronize enables you to transfer data in a flexible, convenient and secure way between directories, databases or files. Manipulate data by applying simple transformations to join fields and add or remove characters; or perform complex conversions by writing your own script to transform data before it gets saved at the destination side. Perform a test run and preview the results before actually executing a transfer and committing changes. Save and schedule your jobs to execute them unattended at a later time.

What's New in GroupID 6.0

Imanami GroupID 6.0 focuses on stability and performance improvements in addition to many new features, all designed around the feedback and suggestions of our valued customers.

Given below are the new features introduced in GroupID 6.0.

Automate

Change Tracking and History Management

This feature enables Automate to keep track of selected GroupID actions and maintains a history of all changes resulting from them. Administrators can choose the actions that they want to be tracked. Changes to directory objects resulting from these actions will be saved in history. The detail in history data can include the old and new values of attributes that were changed during an action.

The history feature can track changes to objects that are made using GroupID Management Console, Self-Service Portals and GroupID Management Shell. Any changes that are made using Active Directory native tools cannot be tracked by GroupID and will not be a part of the history data. See **Group** in **Chapter 9: Managing Groups** and **History Settings** in **Part 7: GroupID Configurations** for detailed information on this.

Security Group Expiration

Security Group Expiration was available as a separate add-on for Automate in GroupID 5.5. With GroupID 6.0, the component has been integrated into Automate.

Password Center

A new addition to the GroupID suite, Password Center (PC) offers a new way for your administrators to save themselves from the mundane tasks of unlocking user accounts and resetting passwords. Use PC to create portals for your network users from where they can carry out these tasks on their own. Create separate portals with respect to domains, directory services, data sources, and departments in your organization; or with respect to any other formation according to your organizational needs. Customize, personalize, localize and secure each portal and make them available to your users through your corporate intranet or the Internet.

With PC, you can do more than just setup portals for password management. You can also extend your Active Directory password policy by applying more conditions that subject passwords to more complexity than that offered by Active Directory out-of-the-box. See **Part 6: Password Center** for detailed information on this.

Self-Service

Change Tracking and History Management

With the new Change Tracking feature in GroupID, Self-Service Portals include new pages and user interface elements for displaying historical changes to Active Directory objects. My History, My Groups History and My Direct Reports history are the new pages in Self-Service Portals that display the history of changes made to the respective objects belonging to a user. A new History tab on the Properties page shows the change history for the selected object.

Import/Export Members and Additional Owners for Groups from Portals

This implementation for Self-Service enables users to import and export, members and additional owners, for groups from the portal. The import and export functions make use of an external file. When importing, this file will be used as the source from which the data will be loaded. Similarly, when exporting, the data will be written to an external file that will be generated automatically.

User-friendly naming for Import/Export Attributes

In order to develop a better and refined understanding of the complex native Active Directory attributes of an object, Management Console now provides options for assigning intuitional and easy to understand titles to them. This concept directly facilitates Import and Export membership process. When these titles appear on the import and export pages of the respective Portal, they help users understand and easily identify the referred Active Directory attribute. For more details, see **Rename Active Directory attributes** in **Chapter 7: Customizing the Portal**.

New display types for multi-value attributes

Self-Service provides new display types for multi-value Active Directory attributes. Prior to this, the textbox display type was available for use with multi-value attributes which prevented the display and entry of multiple values.

The new multi-value display types make use of the list box control and show multiple values at a time. They are also accompanied by a toolbar containing the buttons for adding and removing items from the list. For more information, see **Display Types** in **Chapter 7: Customizing the Portal**.

Synchronize

Inline help for the Global Script Editor

Global Script Editor is made intelligent to sense the script being typed. It displays the list of the members of the current object as the script is typed. Moreover, help for the parameters that are to be passed to the functions is also available now.

UI Optimization

Synchronize job execution from the Management Console is now equally as efficient as from the command-line.

Support for Novell Directory Services as a Destination Provider

Synchronize now supports Novell Directory Services as a destination provider. Synchronizing NDS destinations with the supported source providers will create, update or delete objects on NDS as required.

Launching GroupID

To launch GroupID; point to Windows Programs menu, next point to **Imanami** > **GroupID 6.0** and then click **Group Management Console**.

When you launch GroupID for the first time after installation, you will not be able to use Automate, Self-Service, Synchronize and Password Center modules until you have entered the license number and license key. Reports is a free module and will be available even if you have not entered the license information.

To learn more about licensing GroupID or any of its modules, refer to the **Licensing GroupID** section later in this chapter.

Licensing GroupID

Using a GroupID module will require a license number and a key. For more information on how to obtain a license, see the GroupID Installation Guide.

Once you have obtained the license number and the key, use the following instructions to license the product:

1. From GroupID Management Console, click the **Configuration** node and then click **Modify User Options**.
2. On the **Options** dialog box, click **Licensing** and then click **Add**.
3. On the **Edit License** dialog box:
    i. In the **License number** box, type the license number for your copy of GroupID.
    ii. In the **License key** box, type the key provided by Imanami for your copy of GroupID.
4. Click **OK** and restart GroupID.

The license or licenses entered will show in the **Licenses** list. This list will provide the following information about every license provided:

- **Status** - The expiry date of the license.
- **Number** - This is the license number that you entered.
- **Key** - This is the license key that you entered.
- **Licenses** - The number of computers this license is valid for.
- **Module** - The name of the module this license applies to. If a complete license was purchased, this will show All. Otherwise the name of the particular module will be displayed here.

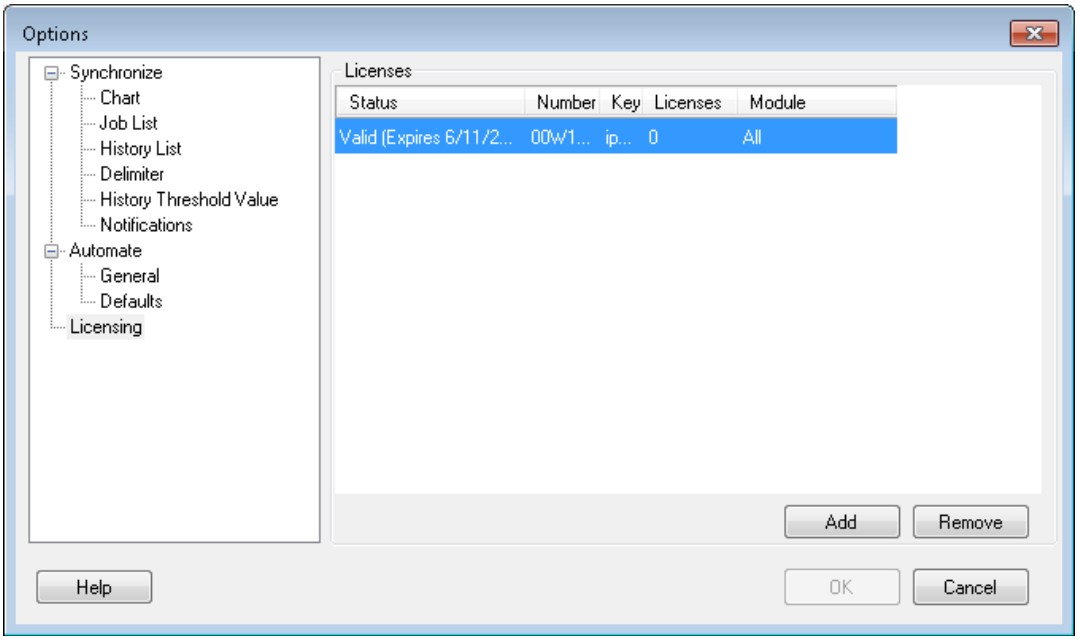


Figure - The Options dialog box

The User Interface

The GroupID user interface is covered in the following sections:

- GroupID Management Console
- The Tree View
- The Action Pane
- The Shortcut Menu
- The Options Dialog box

GroupID Management Console

The GroupID Management Console is a custom Microsoft Management Console with the GroupID snap-in added.

Figure - GroupID Management Console

The Tree View

The left pane of the GroupID Management Console displays the tree view where each node of the tree groups relevant functionality that GroupID offers. If you have added the GroupID snap-in as a part of some custom management console, it might appear as a child node of some other snap-in. You can hide the tree view by clicking **Show/Hide Console Tree** in the GroupID Management Console.

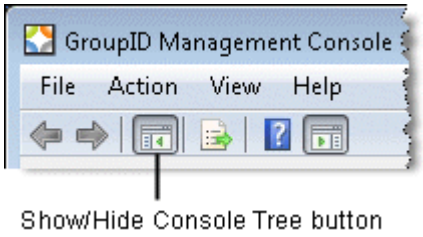


Figure - The Show/Hide Console Tree button

Following is a summary of GroupID nodes available in the tree view:

GroupID node	Description
Getting Started	Shows a brief introduction of GroupID and its modules.
Automate	This node groups the features of Automate. For more information, refer to

GroupID node	Description
	the **Automate** section.
Password Center	This node groups the features of Password Center. For more information, refer to **Password Center** section.
Reports	This node groups the reports that you can run on the Microsoft Exchange and Active Directory. For more information, refer to the **Reports** section.
Self-Service	This node groups the features of Self-Service. For more information, refer to the **Self-Service** section.
Synchronize	This node groups the features of Synchronize. For more information, refer to the **Synchronize** section.
Configuration	This node acts as the control panel for GroupID. From here you can check the status of GroupID services running on your machine. You can also manage scheduled tasks and configure settings for GroupID features and its modules.

The Actions Pane

The right pane of the GroupID Management Console is the **Actions** pane. This pane shows the list of commands that are available for a selected node or item in the tree view or workspace. The commands in the Action pane are also available from the **Actions** menu and the shortcut menu for the selected item. You can hide the pane by clicking **Show/Hide Action Pane** on the GroupID Management Console toolbar.

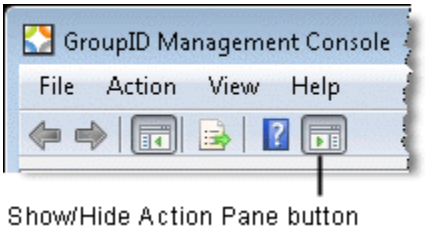


Figure - The Show/Hide Action Pane button

The Shortcut Menu

The shortcut menu appears when you right-click an item in the tree view or workspace. It lists commands pertaining only to the selected item.

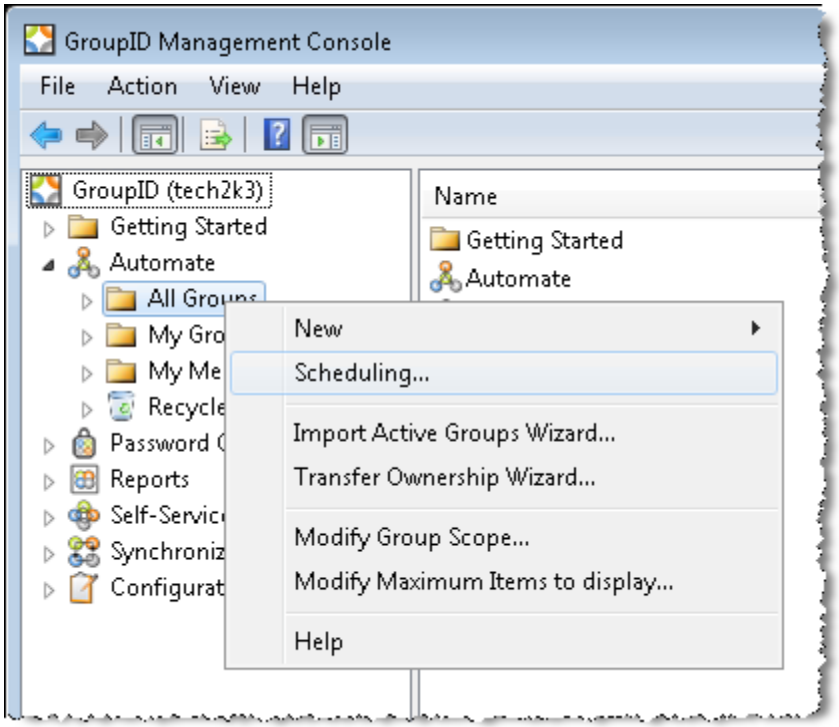


Figure - The shortcut menu for Automate > All Groups node

The Options Dialog box

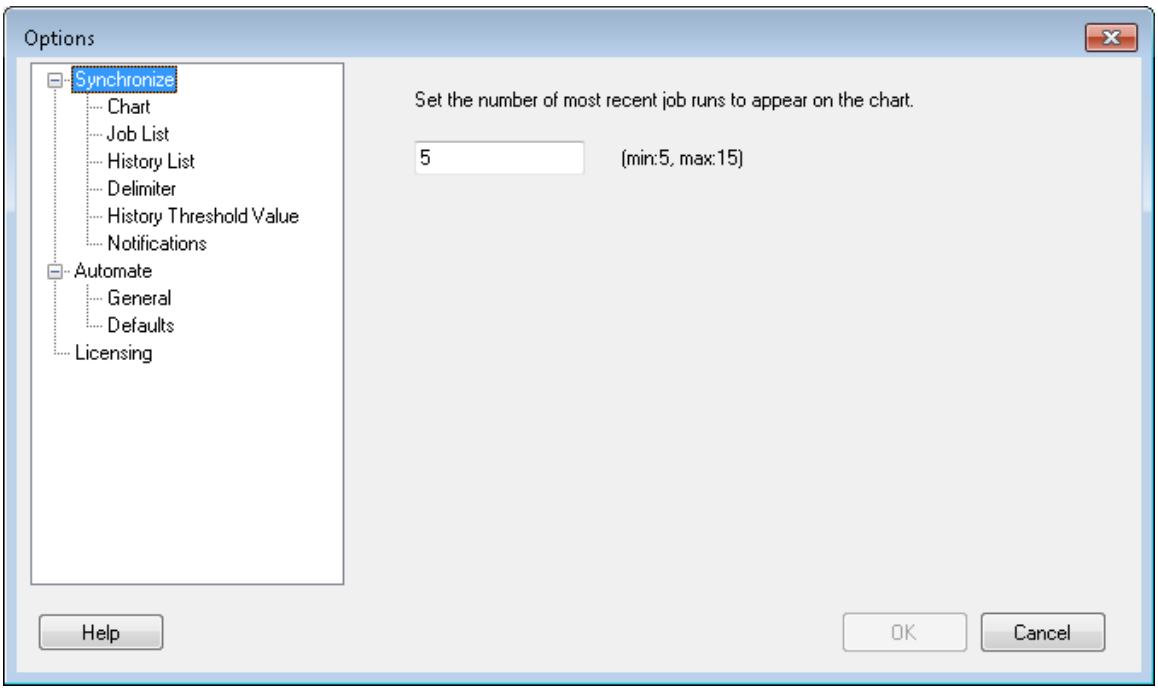


Figure - The Options dialog box

Settings that are specific to Synchronize, Automate and Self-Service modules are available from the **Options** dialog box. This dialog box can be opened by one of the following ways:

- Selecting a module and then clicking the **Options** command on the **Action** menu.
- Right-clicking a module node and then clicking **Options** on the shortcut menu.
- Clicking the **Configuration** node and then clicking **Modify User Options**.

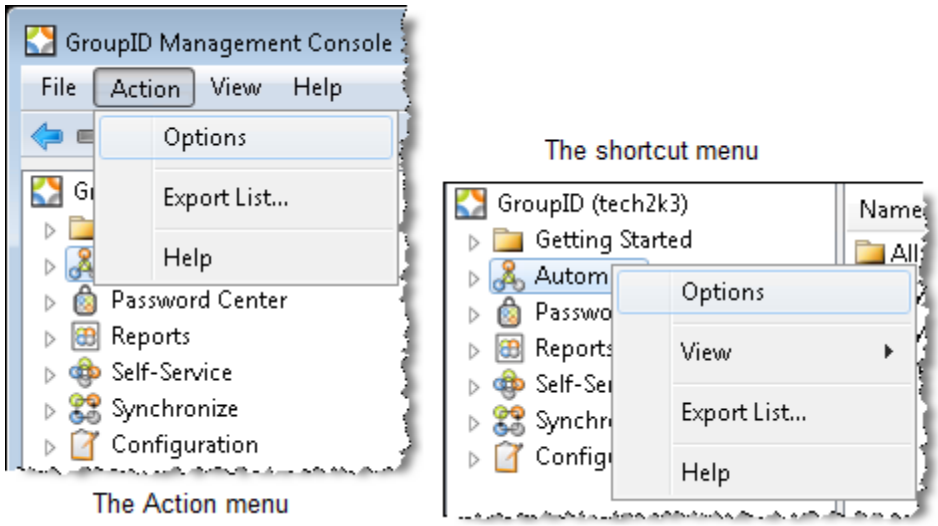


Figure - The Options command on the Action and shortcut menus.

Creating a Service Account for Active Directory and Exchange

Prior to launching GroupID, it is recommended that you add a new service account that has sufficient permissions to Active Directory and Exchange Server objects. Use this service account to connect GroupID to the domain. If you plan to install GroupID on a member server or computer, you will need to add this service account to the membership of the local Administrators group on that machine.

The instructions below list the procedure for creating a service account in Active Directory:

1. Open **Active Directory Users and Computers**.
    - **For Windows Servers**, click Windows **Start** button, click **Programs** (or **All Programs**), point to **Administrative Tools**, and then click **Active Directory Users and Computer**.
    - **For Windows XP**, click Windows XP **Start** button, click **Control Panel**, click **Performance and Maintenance**, click **Administrative Tools** and then double-click **Active Directory Users and Computer**. (The given instructions are for the default Windows XP views. Please refer to Windows Help for instructions on the Classic views.)
    - **For Windows Vista**, click Windows Vista Start button, click **Control Panel**, click **System and Maintenance**, click **Administrative Tools** and then double-click **Active Directory Users and Computer**. (The given instructions are for the default Windows Vista views. Please refer to Windows Help for instructions on the Classic views.)
    - **For Windows 7**, click Windows 7 Start button, click **Control Panel**, click **Administrative Tools** and then double-click **Active Directory Users and Computer**.

2. In the directory tree, right-click the **Users** container, point to **New**, and then click **User**. This will start the wizard for creating a new user.

3. Enter in all required information for the user as you walk through the wizard.

4. As the wizard completes, click the **Users** container and you will see the newly created user in the **Users** list.

To grant permissions to this service account, you can do one of the following:

- Make it a member of one of the following groups:

Recommended	Domain Admins
Minimum	Account Operators

- Delegate it permissions at object level using the **Delegation of Control Wizard** in Active Directory Users and Computers. This method can be used to set the least level of permissions for the service account.

The above steps will create a user account and grant privileges to it for the Active Directory objects. To set permissions on Exchange Server objects for this user, follow the instructions below:

For Exchange Server 2003

1. In the Windows Programs menu, point to **Microsoft Exchange**, and then click **System Manager**.

2. Right-click the organization where you want to delegate permissions, and then click **Delegate control**.
   This starts the Exchange Administration Delegation wizard.

3. On the welcome page of the **Exchange Administration Delegation** wizard, click **Next**.

4. On the **Users or Groups** page, click **Add**.
   This displays the **Delegate Control** dialog box.

5. On the **Delegate Control** dialog box:

   - Click **Browse** and on the **Select Users, Computers, or Group** dialog box:

     - In the **Enter the object name to select** box, type the name of the user you have just created and press **Enter**. This displays the name of the user in the box.

     - Click **OK** to close the dialog box.

   - The minimum permissions required for the service account is **Exchange View Only Administrator** role, so from the **Role** list, select a role accordingly.

   - Click **OK** to close the dialog box. The user or the group that you added appears in the **Users and groups** list.

6. Click **Next** and then click **Finish**.

For Exchange Server 2007

1. In the Windows Programs menu, point to **Microsoft Exchange Server 2007** and then click **Exchange Management Console**.

2. In the console tree, right-click **Organization Configuration** and then click **Add Exchange Administrator**.
   This starts the Add Exchange Administrator wizard.

3. On the **Add Exchange Administrator** wizard, click **Browse** and on the **Select User or Group to Delegate** dialog box:

   - From the list, select the user you have just created.

   - Click **OK** to close the dialog box.

4. The minimum permissions required for the service account is **Exchange Recipient Administrator** role, so from the **Select the role and scope of this Exchange administrator** area, select a role accordingly.

5. Click **Add**.

6. On the **Completion** page; review the summary, and then click **Finish** to close the Add Exchange Administrator wizard.

For Exchange Server 2010

- Launch the Exchange Management Shell and type the following command:

```
Add-RoleGroupMember  "Recipient Management" -Member domain name\user
```

Connecting to a Domain

Launching GroupID for the first time after a new installation will connect you to your current domain using the credentials of the user account you are logged on with. You can provide the credentials of a different user account for connecting to the domain. It is recommended that you create a new user account for connecting GroupID to a domain. For more information about creating this account, see **Creating a Service Account for Active Directory** earlier in this chapter. You can also configure GroupID to connect to other domains within your current forest, if required.

The instructions below guide you on how to connect GroupID to a domain:

1. Launch the GroupID Management Console.

2. On the tree view, right-click the **GroupID** node and then click **Connect to Domain**.

3. On the **Connect to Domain** dialog box, provide the following information:

   i. Click **Browse** to select the domain you want to connect to. Remember, GroupID only allows you to select domains from your current forest.

   ii. Select the **Connect to server as** check box if you need to connect to the server with different user credentials other than those you are logged on with. Selecting the check box will make the **Authentication** section visible. Provide the following information in this section to use for logging on to the selected server:

      a. In the **User** box, type the user name of account with which to connect.

b. In the **Domain** box, type the domain in which the specified user name exists.

c. In the **Password** box, type the password for the specified user.

iii. You can select the **Save this domain setting for the current console** check box if you want GroupID to use these domain settings every time it is launched.

iv. Click **OK** to close the dialog box.

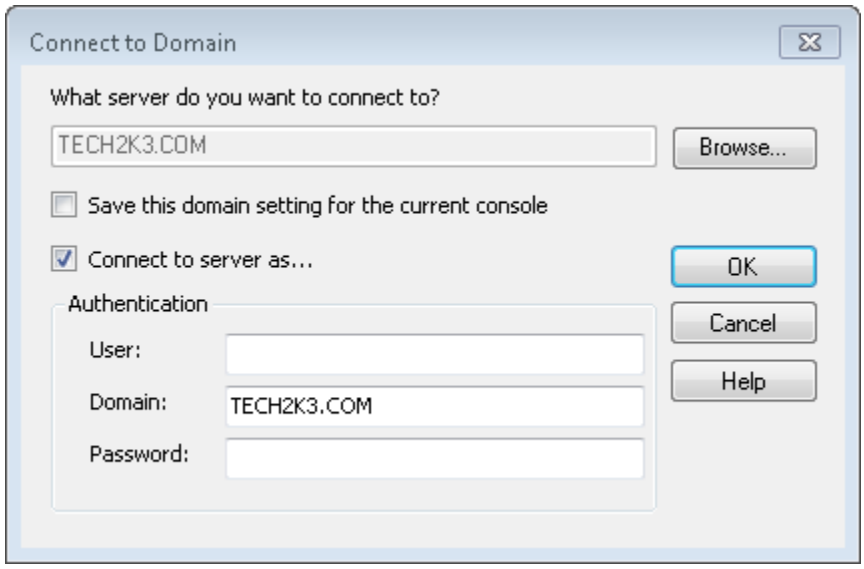


Figure - The Connect to Domain dialog box

Chapter 2: Group Management Concepts

This chapter explains concepts that are critical to understanding the features and functionalities of GroupID. These concepts can be grouped into the following broad categories.

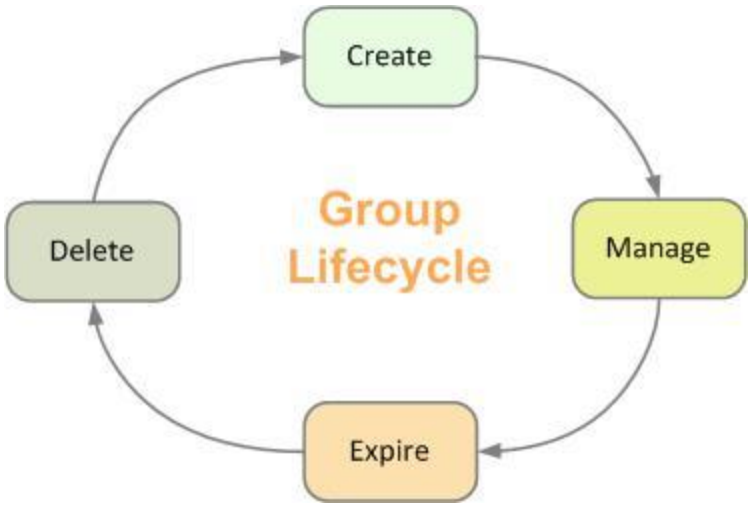
- Group
- Group
- Group
- Security Type
- Group
- Group

Group Lifecycle Management

Accurate Group management is essential to every enterprise to improve productivity and enhance security in terms of granting correct access privileges to appropriate users.

The concept of Group Lifecycle is to devise a process for better management of directory resources. Group Lifecycle is a process that starts with the creation of a group and ends when the group is deleted or removed from the directory. The need for Group Lifecycle Management arises from the problems that organizations face in terms of managing their groups. Groups serve different purposes within an organization. However, the need for all these groups is not necessarily for a life time. Some groups are required for a limited period of time; however, due to the lack of available tools for monitoring groups and their usage activities some of these groups drop off the radar of attention until they start causing problems for the administrator.

GroupID supports the concept of Group Lifecycle Management by providing features to allow control and management of groups from cradle to the grave. Administrators can manage group memberships dynamically when changes occur within the organization. So many changes can happen in an organization that will affect the lifecycle of a group, such as: project teams disbanded, departments reorganized, and company closures which happen on a regular basis in some organizations. GroupID allows IT managers or group owners to set policies that will automatically expire and delete groups from the source directory on a scheduled basis, hence keeping your directory clean and preventing group glut. If an expired group is needed again, you can simply renew it to restart its lifecycle.



Group Classification

GroupID classifies groups into two broad categories i.e. Unmanaged and Managed.

Unmanaged Groups

An unmanaged group is a group you would normally create using Active Directory Users and Computers. Though such groups can be created using GroupID Automate and Self-Service modules, GroupID will not support dynamic updates to them. Any changes to the membership will have to be updated manually.

Managed Groups

A managed group (also known as SmartGroup) is one that dynamically maintains its membership based on rules. These rules are applied in the form of a user-defined LDAP query. You are required to define the rule once and then you can schedule it. When the scheduled task runs, it will apply the defined rule to update the group's memberships. This automated group management allows administrators to easily maintain large distribution lists and security groups without having to manually add or remove members.

SmartGroups can be created and managed through GroupID Automate.

Security Types

Security types indicate the access level for a group. Private, Semi-Private, Semi-Public and Public are the four security types provided by GroupID.

Private

A group that is not available to everyone. Members of such a group are determined by the group owner and they cannot leave a group on their own unless the owner removes them. Requests for joining or leaving such a group cannot be sent.

Semi-Private

Similar to a private group except that members can send requests for joining or leaving the group.

Semi-Public

Similar to a public group except that an e-mail notification is sent to the group owner whenever a member joins or leaves the group.

Public

A public group is open to all users. Users can join and leave a public group without requiring any permission.

Group Types

Active Directory divides groups into two types based on their usage criteria: Distribution Groups and Security Groups. You can use distribution groups to create e-mail distribution lists and security groups to assign permissions to shared resources. A detailed description of these group types is as follows:

Distribution Groups

Distribution groups can be used only with e-mail applications (such as Exchange) to send e-mails to a group of users. Distribution groups are not security-enabled, which means that they cannot be listed in discretionary access control lists (DACLs). If you need a group for controlling access to shared resources, create a security group.

Security Groups

Use with care, a security group can provide an efficient way to assign access to resources in your network. Using security groups, you can assign user rights to security groups in Active Directory and assign permissions to security groups on resources.

Group Scope

Any group, whether it is a security group or a distribution group, is characterized by a scope that identifies the extent to which the group is applied in the domain tree or forest. The boundary, or reach, of a group scope is also determined by the domain functional level of the domain in which it resides. There are three group scopes: universal, global, and domain local.

Universal Groups

Use groups with universal scope to consolidate groups that span domains. To do this, add the accounts to groups with global scope, and then nest these groups within groups that have universal scope. When you use this strategy, any membership changes in the groups that have global scope do not affect the groups with universal scope.

Do not change the membership of a group with universal scope frequently, because any changes to the group membership will cause the entire membership of the group to be replicated to every global catalog in the forest.

Global Groups

Use groups with global scope to manage directory objects that require daily maintenance, such as user and computer accounts. Because groups with global scope are not replicated outside their own domain, you can change accounts in a group having global scope frequently without generating replication traffic to the global catalog.

All rights and permissions assignments are valid only within the domain in which they are assigned. If you apply groups with global scope uniformly across the appropriate domains, you can consolidate references to accounts with similar purposes. This simplifies and rationalizes group management across domains.

It is strongly recommended that you use global groups or universal groups instead of domain local groups when you specify permissions on domain directory objects that are replicated to the global catalog.

Domain Local Groups

Groups with domain local scope help you define and manage access to resources within a single domain. For example, to give five users access to a particular printer, you can add all five user accounts in the printer permissions list. If, however, you later want to give the five users access to a new printer, you must again specify all five accounts in the permissions list for the new printer.

Group Deletion

The concept of deleting groups can be classified as Physical Deletion and Logical Deletion based on the way GroupID handles deleted groups.

Physical Deletion

This involves deleting of groups interactively using the command available from the shortcut menu and the Actions menu. When the user deletes a group manually, GroupID moves it to the **Recycle Bin** stripping most of the properties from the group. The group resides in the Recycle Bin until it is restored. The restoration process is efficient enough that it not only restores the group to the container from where it was deleted but it also reinstates the home container for the group, if deleted.

Logical Deletion

Groups that are deleted by the Group Management Service are classified as logically deleted. The service deletes expired groups automatically based on the deletion interval set for expired groups in global configurations. Logically deleted groups have their names beginning with the **Deleted**_ prefix and are listed under the **Expired Groups** node until renewed or physically deleted.

Part 2 - Self-Service

This part of the documentation covers the Self-Service module of GroupID. It explains how Self-Service Portal is setup and customized according to your enterprise needs. Information about Workflows and their implementation is also included.

Chapter 3: Introduction, introduces you to Self-Service, its features and the user interface elements.

Chapter 4: Setting Up a New Portal, provides instructions on setting-up a new Portal.

Chapter 5: Portal, explains how to configure Portal settings according to your requirements.

Chapter 6: Workflows, gives an overview of Workflows and how they are used in Self-Service

Chapter 7: Customizing the Portal, provides instruction on applying different customizations to the Web Portal interface.

Chapter 3: Introduction

This chapter provides a brief overview of Self-Service and its key features. The software requirements and their installation instructions are also incorporated. This chapter also helps you to get familiarized with Self-Service user interfaces. The chapter is divided into following sections:

Self-Service, provides a brief overview of Self-Service.

Features, describes the key features of Self-Service.

Requirements for Self-Service, covers software requirements for Self-Service.

Self-Service, introduces you to the Self-Service interfaces in the management console and the appearance of Web Portal in different functionality modes.

Self-Service - Overview

Self-Service - a simple yet powerful Web-based directory and group management solution - provides quick wins in Identity Management projects by empowering enterprise users to serve themselves in terms of managing their own directory information. The enterprise user is the key to providing accurate and reliable data, since they are the primary source of information. By empowering enterprise users to maintain and update their own information it will free up time for administrators to address more important enterprise challenges.

At the same time administrators maintain complete control to enforce data integrity. Administrators can control which information the user can update and what information can be viewed. Administrators can also reduce the work that is required to manage groups. Self-Service allows the end users to create, delete and edit public, semi-public and private groups, without any time being required from an administrator.

Features

Group Management

The Group Management feature allows users to create, delete and manage their own groups. Users are also allowed to join and leave groups based on the security settings of that group without requiring any support from the administrator. Users can expire and renew groups under the complete supervision and control of the administrator.

Workflow Management

Self-Service has a built-in auditing system to ensure that correct data is entered before applying changes in Active Directory. Using Workflows, Administrators can control specific fields to be submitted for approval before changes are made to the directory. They have the authority to accept or reject these approval requests to ensure the data integrity.

Enterprise Phone Directory

The phone book feature allows anonymous or authenticated read-only access to the directory. You can search on multiple fields and even export the results to a Microsoft Excel file. Self-Service phone book supports WAP devices, such as BlackBerry and cell phones.

Add Photos to Employee Profiles

It is helpful if you can see a picture of a coworker when viewing their information in a directory. Now you can easily identify them walking down the hall towards you. This is a great feature to have for any environment where you need to know what someone looks like for security purposes. Self-Service extends the capability of your directory by providing support for integration of employee photographs within their profiles.

Role-based Security

Assign roles to users based on the permissions they should have to each section of a Portal. Customize the pre-defined roles: End-user, Helpdesk and Administrator; to lock down specific fields or tabs used to view or modify users, contacts or groups within the Portal.

SharePoint Integration

Allow your users to launch Self-Service directly from SharePoint by tunneling end-users through your corporate portal for essential information. You can easily integrate Self-Service into SharePoint by creating a Web Part and then publishing the site to enable users to gain access to it.

Requirements for Self-Service

Self-Service requires Microsoft Internet Information Server (IIS) 6.0 or higher for Portal creation. The IIS is Microsoft's implementation of a Web server for the Windows platform. IIS should be installed on the same machine where GroupID is installed. For information about installing IIS, see **Installing IIS** in the GroupID Installation Guide. Self-Service can optionally be installed on an Active Directory domain controller.

Before installing Self-Service, you should determine which Active Directory domains you will be using with Self-Service. Active Directory domain controllers can only modify objects in their domain or forest.

If you have multiple Active Directory domains you want to use with Self-Service, you have a choice to make:

- A Self-Service Portal for each domain on the same machine
- A single Self-Service Portal for a single Active Directory forest

While making a decision, consider bandwidth between the proposed server for installing Self-Service and the Active Directory domain controller responsible for the target domain. If there is little available bandwidth between the Active Directory domain controller and the proposed server then you should install Self-Service on an IIS closer to a server in the target domain or Exchange site.

Self-Service User Interfaces

Self-Service provides two user interfaces for directory and group management:

- Self-Service Administrator
- Web Portal

Self-Service Administrator

The Administrator interface - the **Self-Service** node in the tree view of GroupID Management Console - enables administrators to monitor and control the overall configuration of Self-Service Portals. Administrators can create new Portals, apply restrictions, control user actions by implementing Workflows and customize the Portal appearance.

Web Portal

This is the interface that is available to the end users after the Administrator has created and configured the Portal. The Web Portal allows users to carry out certain tasks based on the features set by the administrator. These features are set using the functionality mode setting.

Self-Service in GroupID Management Console

In GroupID Management Console, **Self-Service** node appears below **Reports**. From here, you can establish and manage virtual links (referred as Portals) with the Active Directory domain controller that network users utilize for managing directory information. Expand the Self-Service node to view its sub-nodes. The sub-nodes of Self-Service allow you to control the configuration of your Self-Service Portals and manage the Workflow requests that you have sent or received. Right-clicking a node at any level, including the Self-Service node itself, will display the shortcut menu with commands that you can execute at that level.

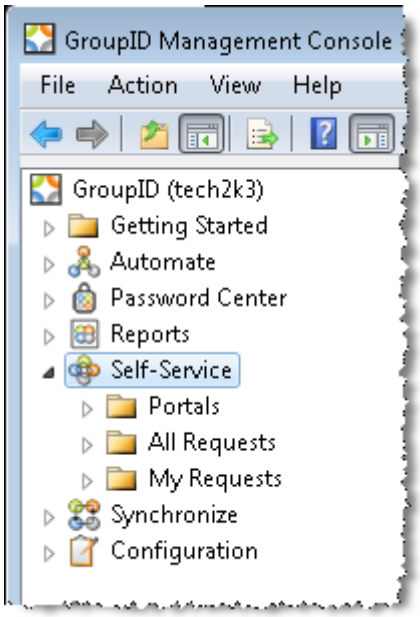


Figure - The Self-Service node

Following is a summary of the Self-Service sub-nodes:

Sub-node	Description
Portals	Shows the list of existing Self-Service Portals. Each Portal has a Server and Design configuration associated with it that controls the Portal and its appearance settings respectively.
All Requests	Shows list of all Workflow requests generated by the enterprise users through different Self-Service Portals created on your machine. For more information on Workflow requests, see **Chapter 6: Workflows**.
My Requests	Shows the list of all Workflow requests that have been generated by you from different Self-Service Portals created on your machine. The list includes both pending and processed requests. For more information on Workflow requests, see **Chapter 6: Workflows**.

Self-Service Functionality Modes

Self-Service functionality modes allow you to tailor the user experience by exposing only the functionality required. These functionality modes limit the overall functionality of the Self-Service Portal available to the users. Self-Service supports five functionality modes. These are:

1. Enterprise
2. My Profile
3. Update Wizard
4. Groups
5. Phonebook

Enterprise Mode

This is the default functionality mode of a Portal when it is created. The Enterprise mode exposes all functionality of the Self-Service Portal including searching the directory, updating personal information, managing groups or memberships, managing groups' life cycle, or controlling Workflow requests and administration.

The figure below shows the Self-Service Portal in Enterprise mode.

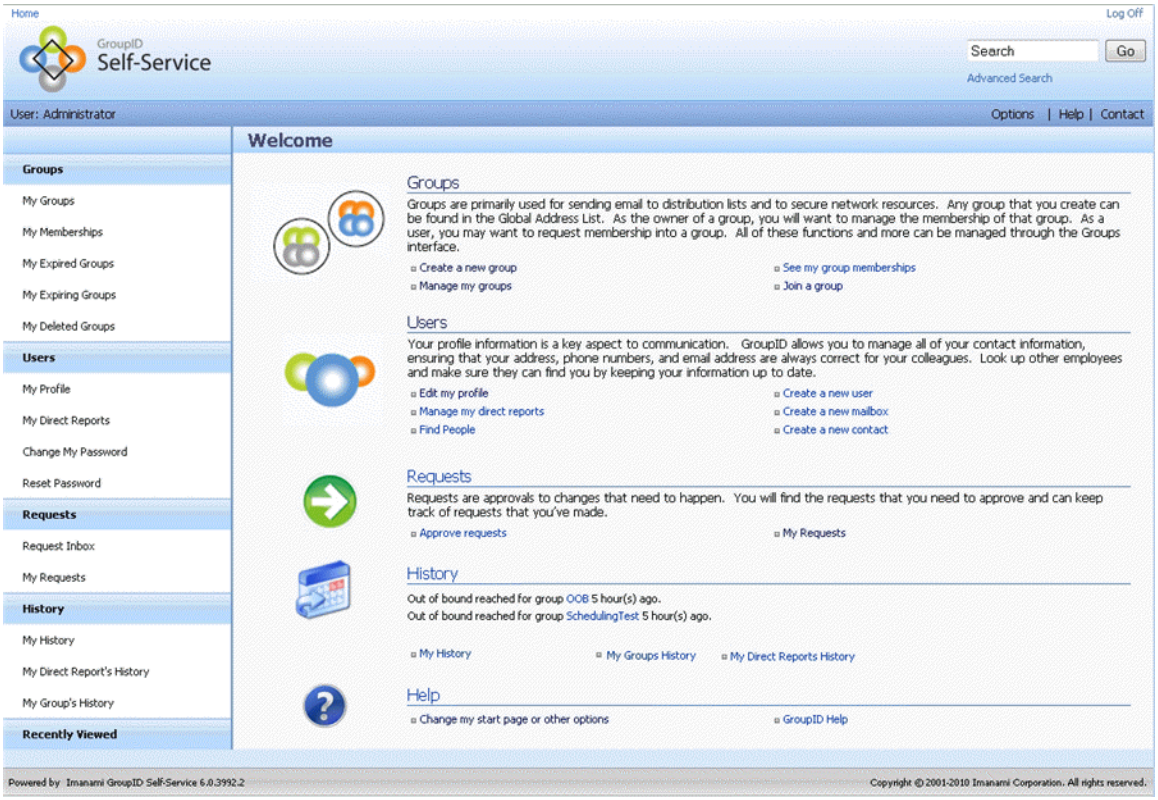

Home
Log Off
GroupID
Self-Service
Search
Go
Advanced Search
User: Administrator
Options | Help | Contact
Welcome
Groups
My Groups
My Memberships
My Expired Groups
My Expiring Groups
My Deleted Groups
Users
My Profile
My Direct Reports
Change My Password
Reset Password
Requests
Request Inbox
My Requests
History
My History
My Direct Report's History
My Group's History
Recently Viewed
Groups
Groups are primarily used for sending email to distribution lists and to secure network resources. Any group that you create can be found in the Global Address List. As the owner of a group, you will want to manage the membership of that group. As a user, you may want to request membership into a group. All of these functions and more can be managed through the Groups interface.
Create a new group
Manage my groups
See my group memberships
Join a group
Users
Your profile information is a key aspect to communication. GroupID allows you to manage all of your contact information, ensuring that your address, phone numbers, and email address are always correct for your colleagues. Look up other employees and make sure they can find you by keeping your information up to date.
Edit my profile
Manage my direct reports
Find People
Create a new user
Create a new mailbox
Create a new contact
Requests
Requests are approvals to changes that need to happen. You will find the requests that you need to approve and can keep track of requests that you've made.
Approve requests
My Requests
History
Out of bound reached for group OOB 5 hour(s) ago.
Out of bound reached for group SchedulingTest 5 hour(s) ago.
My History
My Groups History
My Direct Reports History
Help
Change my start page or other options
GroupID Help
Powered by Imanami GroupID Self-Service 6.0.3992.2
Copyright © 2001-2010 Imanami Corporation. All rights reserved.

Figure - Self-Service Portal in the Enterprise mode

My Profile Mode

This functionality mode exposes the ability to allow users to update their own profile. The profile information will include name, department, designation, contact information and so on. This mode does not support anonymous access, directory searches or overriding the default start page.

The figure below shows the Self-Service Portal in My Profile mode.

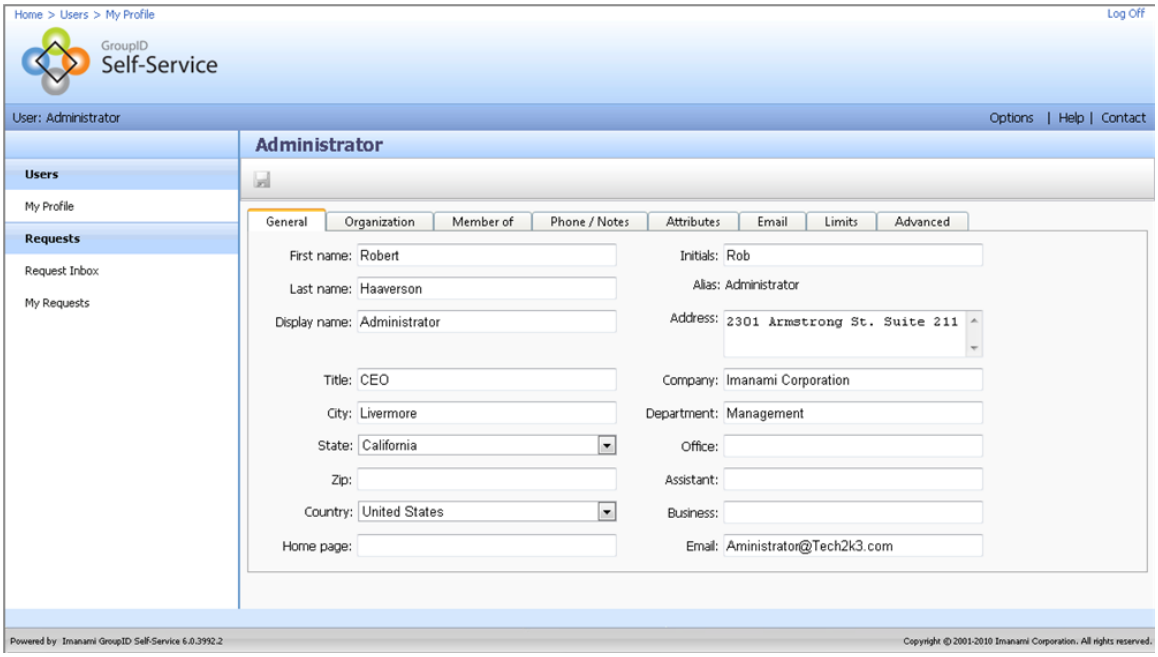


Figure - Self-Service Portal in My Profile mode

Update Wizard Mode

This mode provides the same functionality as **My Profile** mode. The only difference between the two modes is the approach these provide for profile update. Update Wizard mode allows users to update their profile information using a wizard. Similar to My Profile, this mode does not support anonymous access, directory searches, or overriding the default start page.

The figure below shows the Self-Service Portal in Update Wizard mode.

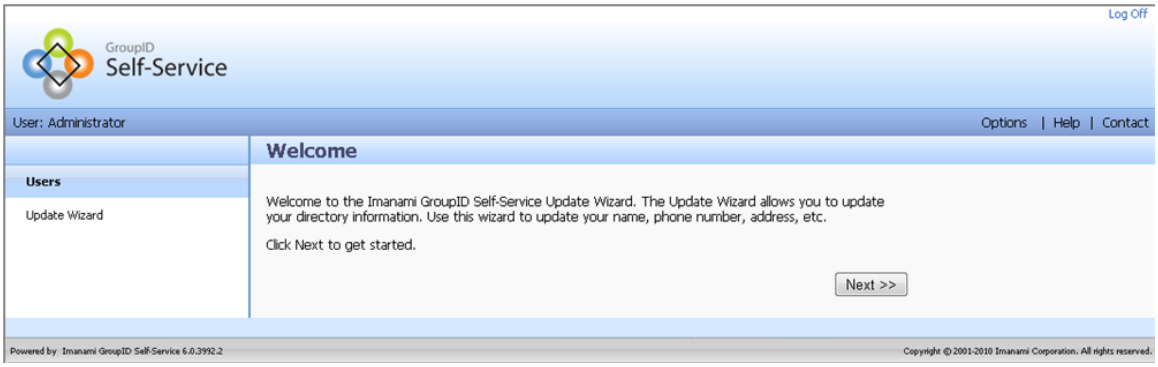

Log Off
GroupID
Self-Service
User: Administrator
Options | Help | Contact
Welcome
Users
Update Wizard
Welcome to the Imanami GroupID Self-Service Update Wizard. The Update Wizard allows you to update your directory information. Use this wizard to update your name, phone number, address, etc.
Click Next to get started.
Next >>
Powered by Imanami GroupID Self-Service 6.0.3992.2
Copyright © 2001-2010 Imanami Corporation. All rights reserved.

Figure - Self-Service Portal in the Update Wizard mode

Groups Mode

This mode exposes the ability to manage groups, group memberships, and group life cycle policy. You can manage the Workflow requests that you have received for approval and can view the requests sent by you. You can also customize different display options for the Portal which enables you to fine-tune the Portal appearance according to your preferences.

The figure below shows the Self-Service Portal in Groups mode.

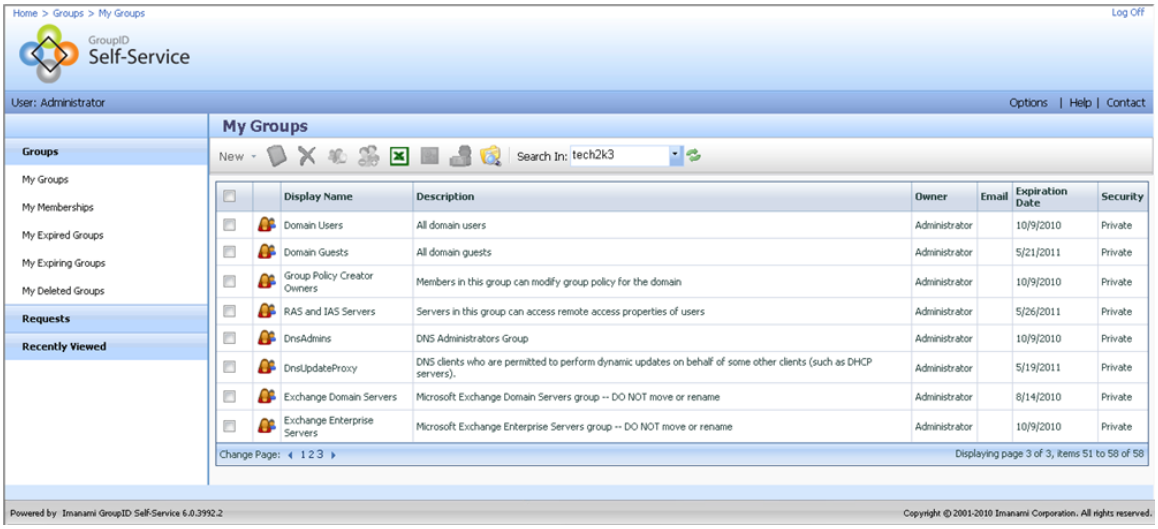


Figure - Self-Service Portal in Groups mode

Phonebook Mode

This mode exposes the ability to search the directory and view the information for directory users, groups, contacts and folders. The Phonebook mode is read-only and users are not allowed to change any information.

The figure below shows Self-Service Portal in Phonebook mode.

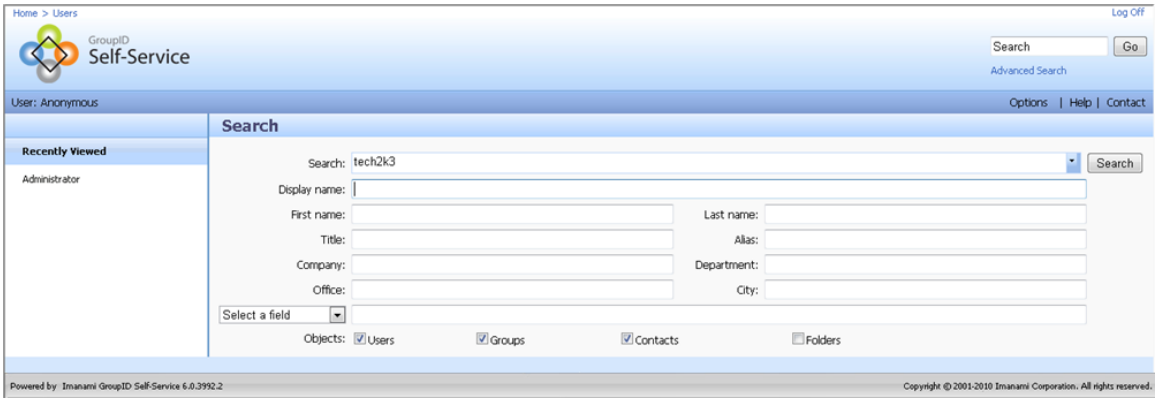


Figure - Self-Service Portal in Phonebook mode

Functionality Modes URLs

Configuring the functionality mode of a Self-Service Portal configures all users that exist in the domain with the same level of access to the Portal. In the Enterprise mode, this might provide extra privileges to the normal user, or in any other functionality mode, deprive the administrators of their rights.

A certain group of users can be made to access the Portal in a specific functionality mode, while keeping the Portal configured in another functionality mode, by providing the users with the respective functionality mode address.

The Enterprise mode (also the default functionality mode of the Portal), on the **Server** node under the **General** tab, displays the addresses for all functionality modes. For any other functionality mode, only its respective address displays on this tab.

The following table shows the addresses (URLs) for all functionality modes:

URL	Description
http://*Server*/*PortalName*	Provides access to the Enterprise mode.
http://*Server*/*PortalName*/myprofile	Provides access to the My Profile mode only.
http://*Server*/*PortalName*/update	Provides access to the Update mode only.
http://*Server*/*PortalName*/groups	Provides access to the Groups mode only.
http://*Server*/*PortalName*/phonebook	Provides access to the Phonebook mode only.

Where *Server* is the name of the Web server hosting the Portal; and *PortalName* is the name of your Self-Service Portal.

Chapter 4: Setting Up a New Portal

This chapter provides information on setting up a new Portal. It also explains how to use the functionality modes to limit and control the functionality exposed to the enterprise users. The chapter is divided into the following sections:

Create a new Portal, provide instructions on how to create a new Self-Service Portal.

Duplicate a Portal, explains how to create a Portal by duplicating the configuration of an existing Portal.

Setting Functionality Mode, explains how to use the functionality modes to limit the functionality of Web Portal for the enterprise users according to their privileges.

Create a new Portal

A Portal represents a virtual link with the Active Directory domain controller for which you want to empower enterprise users to manage the directory information. You can create the Portal and configure it according to your enterprise needs.

Prior to creating a new Portal, you will need to add a new Portal Service account that has administrative access to all domain objects. The recommended permission to give to the service account is **Domain Admin** in Active Directory. It is also recommended that you create the user account prior to creating any Portals.

Follow the instructions provided below to create a new Self-Service Portal:

1. If not already open, launch GroupID Management Console.
2. Under the **Self-Service** node, right-click the **Portals** node and click **Create**. GroupID displays the **GroupID-Self Service Portal** dialog box.
3. In the **Server name** box, type the name of your Portal or leave the default name and click **OK**. This will start the wizard for creating a new Portal.

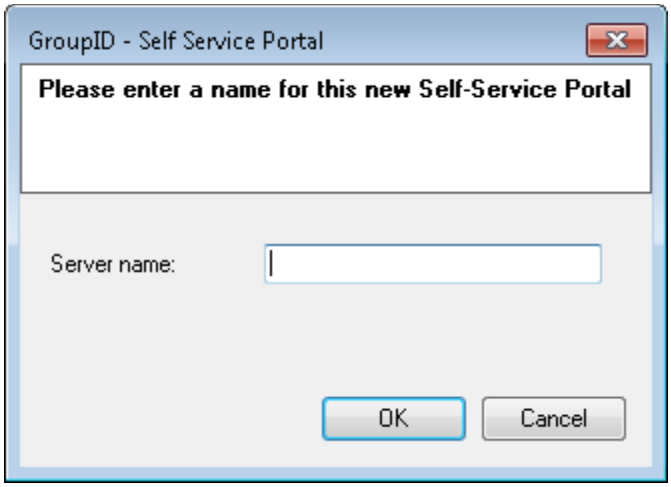


Figure - The GroupID - Self Service Portal dialog box

4. On the welcome page of the wizard, read the welcome message and click **Next**.

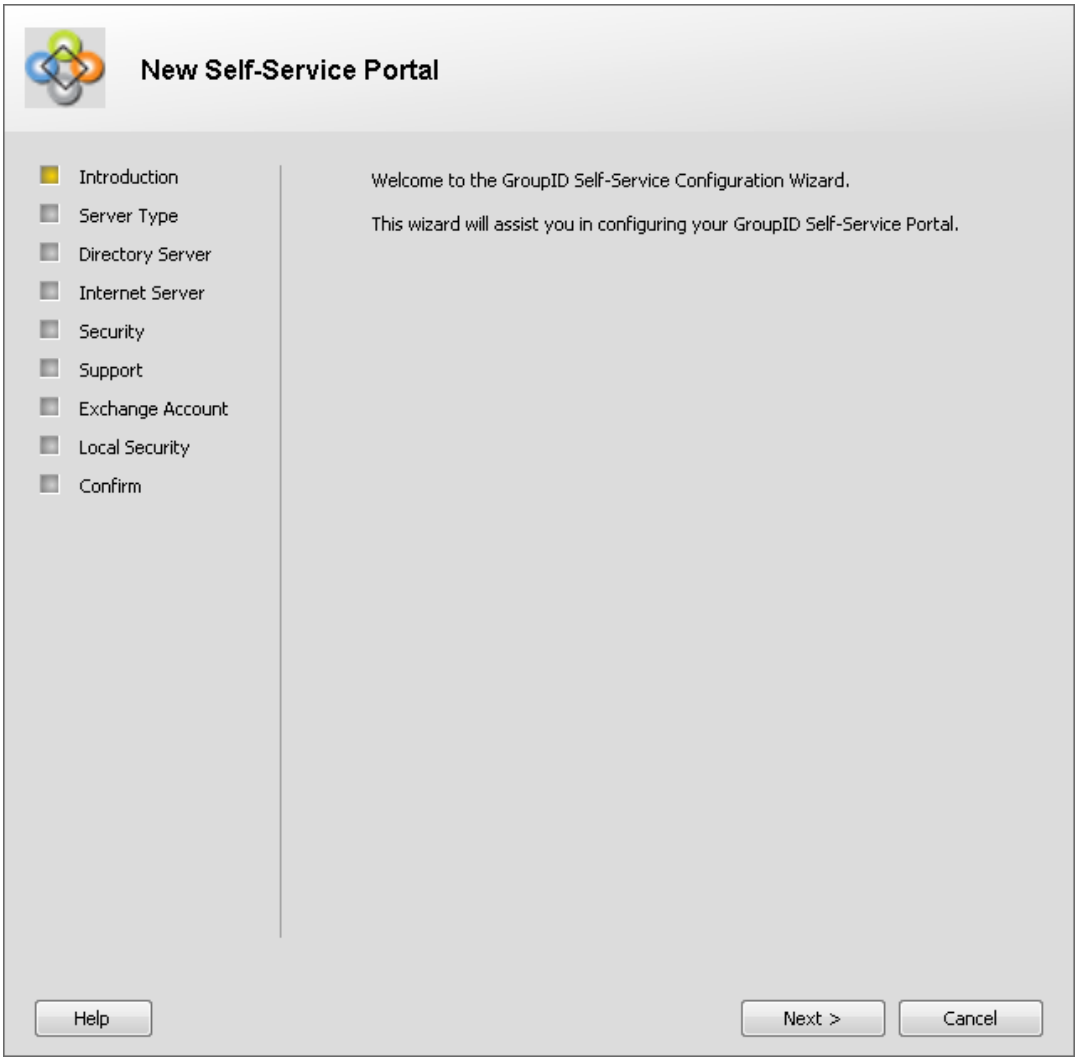


Figure - The welcome page

5. On the **Server Type** page, select the type of server that Portal will connect to. From the list, select:

    - **Active Directory Only**, if the Portal is to connect and communicate only with an Active Directory server or if Exchange is installed in a resource forest.

    - **Active Directory w/Exchange 2003/2007/2010**, if the Portal is to connect and communicate with both Active Directory and Exchange on a Windows server.

6. Click **Next**.

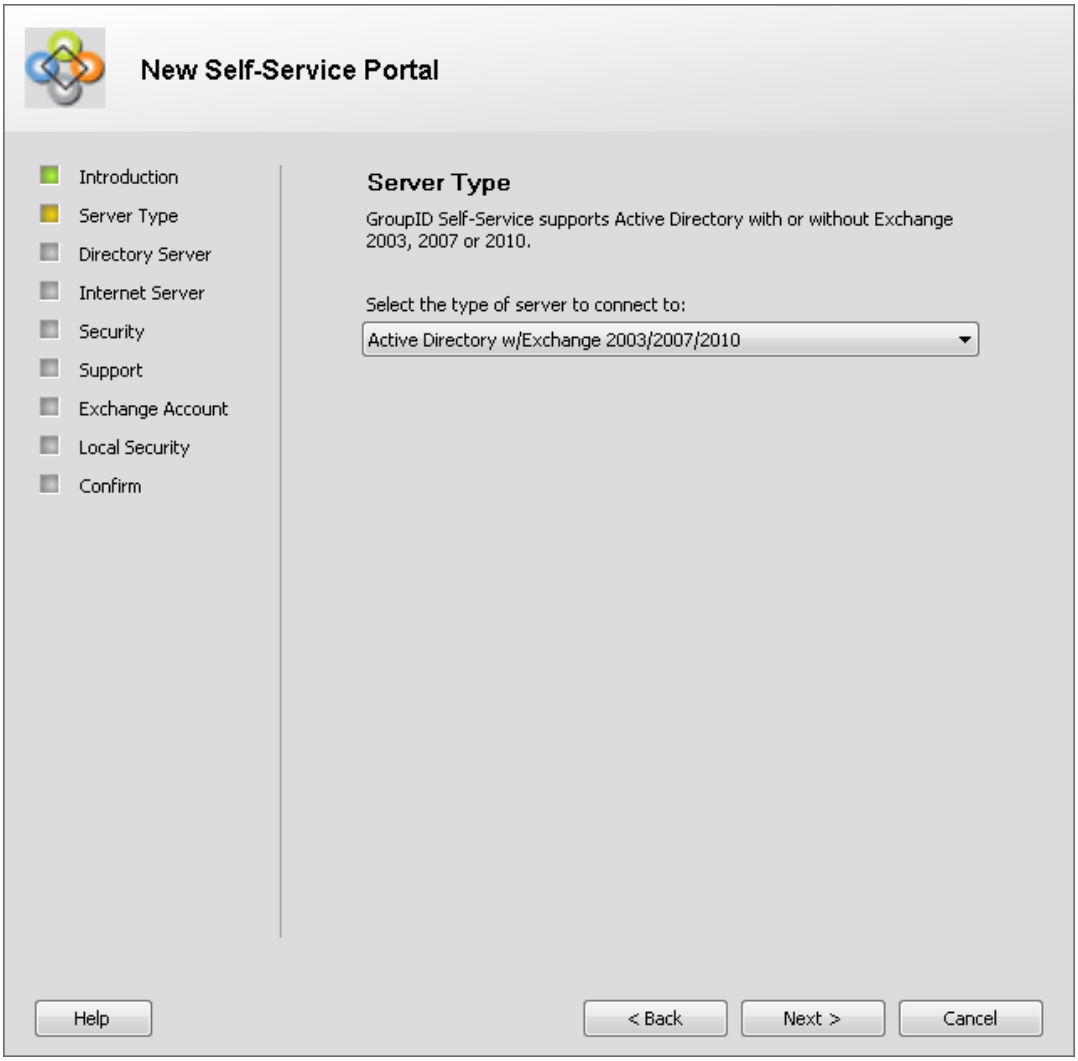


Figure - The Server Type page

7. On the **Directory Server** page, type the information for the given fields:

    i. In the **DNS Domain Name** box, type the name of the DNS domain that Portal will connect to. By default, this box displays the domain controller name of the machine on which it installs.

    ii. In the **Username (domain\user)** box, type the user name of the account used to log on to this domain.

    iii. In both the **Password** boxes that follow, type the password for your specified user account on this domain. The passwords are collected twice as a part of validation to ensure that you typed the intended password correctly.

    iv. Select the **Blank Password** check box to set a blank password for the specified user account. This will also make both the password boxes on this page unavailable. (Not recommended)

8. Click **Next**.

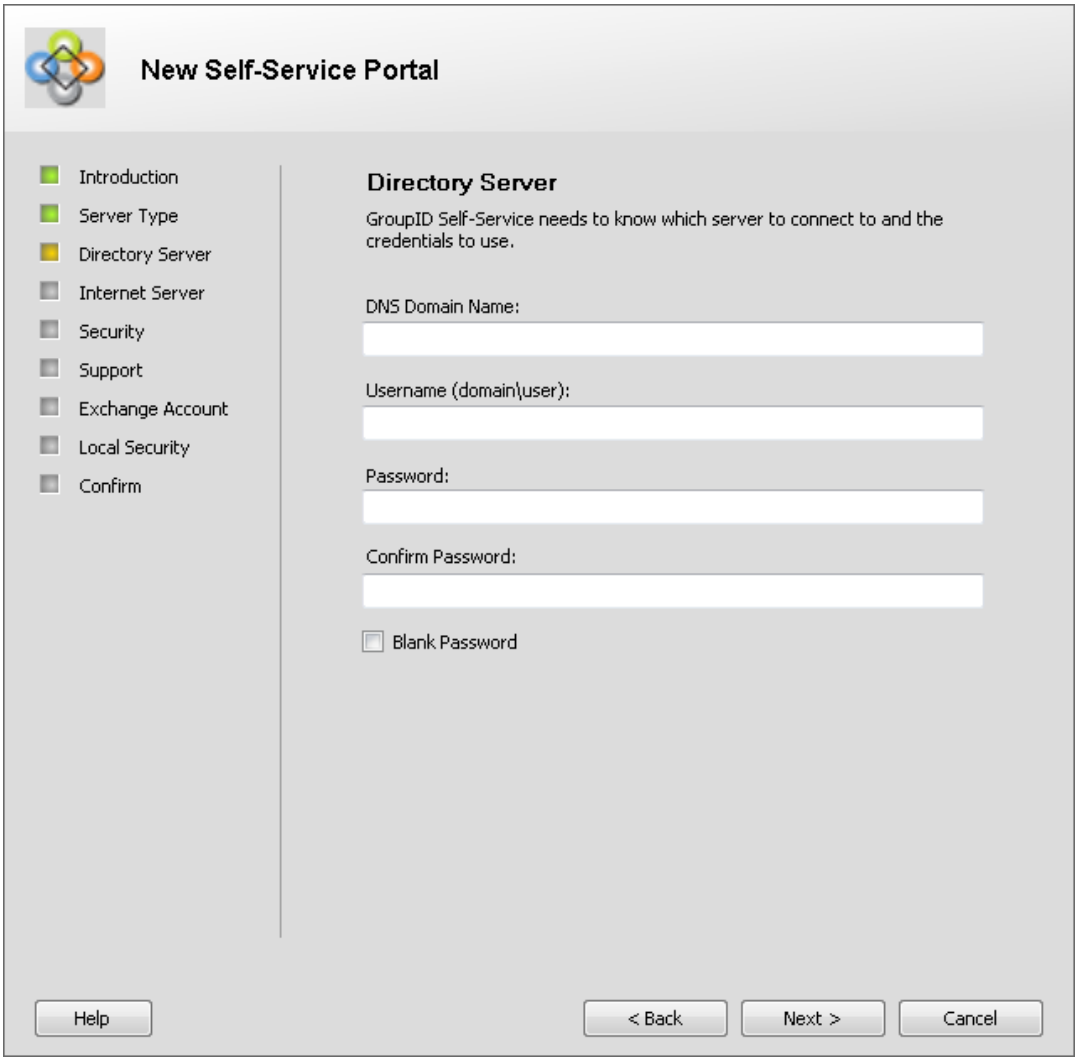


Figure - The Directory Server page

9. On the **Internet Server** page, you make settings for the IIS virtual directory that will host the Portal files. On this page:

    i. The **Path to Portal files** displays the path to the directory where the Portal files are located on disk.

    ii. The **IIS Server** list shows the Web sites defined on a local IIS server. From the list, select the Web site where you want to host the Portal files. The default selection in the list is the default Web site that IIS creates automatically when it is installed.

    iii. From the **Select default language** list, select your default language. The default selection for this is English.

10. Click **Next**.

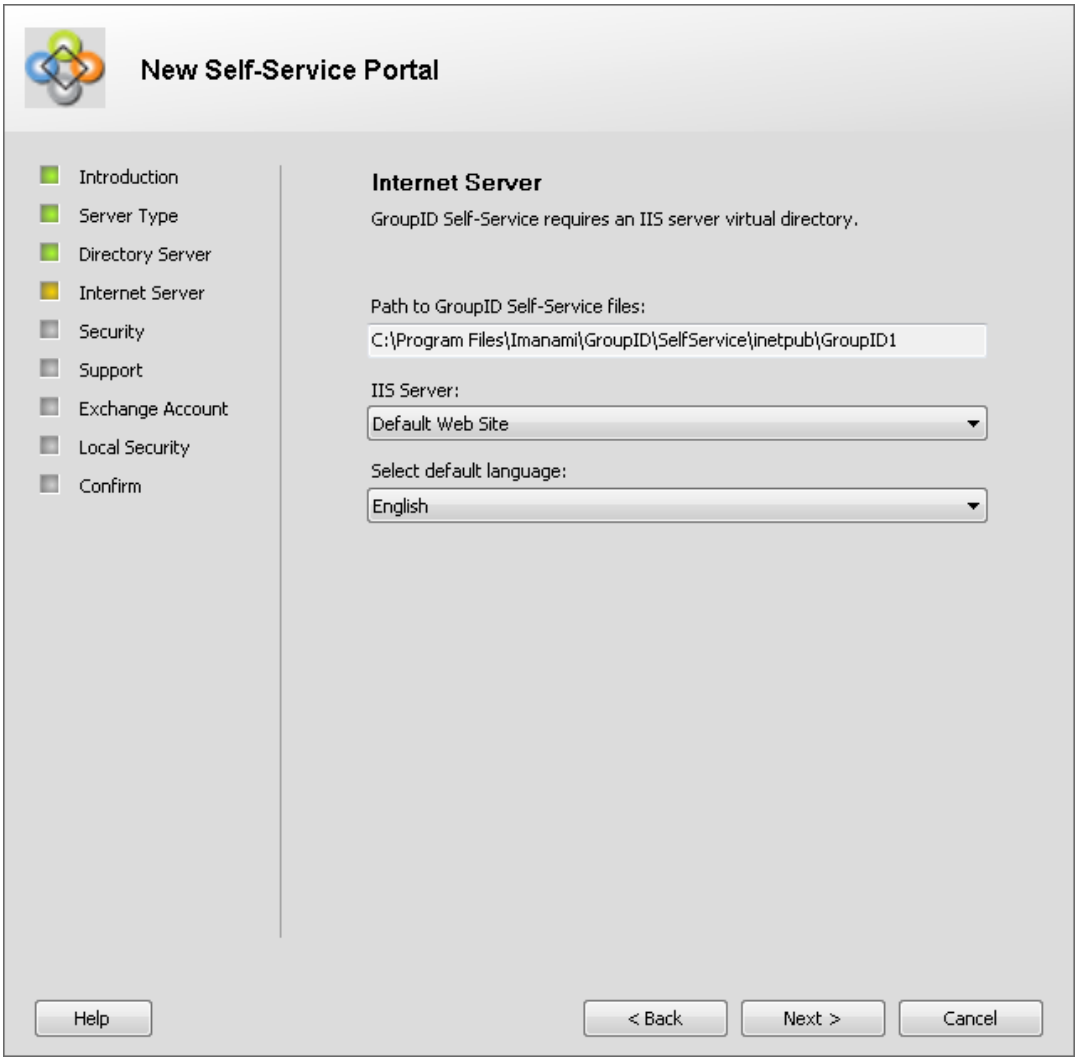


Figure - The Internet Server page

11. On the **Security** page, you configure the security settings for the Portal. Set the fields given on this page as explained in the following steps:

    i. In the **Default Windows Account Domain** box, type the name of a Windows domain that you want to set as the default account domain for authenticating users.

    ii. To set a **HelpDesk Group**:

        a. Click the ... button.

        b. On the **Select Recipients** dialog box, enter the name of an Active Directory group that you would like to set as the helpdesk group.
        If your entered name results in multiple matches, a **Multiple Names Found** dialog box will be displayed for you to select the correct item.

        c. Click **OK**.

    iii. To set an **Administrators Group**, follow the same steps as given for setting a HelpDesk Group.

iv. Select the **Allow anonymous users to log on** check box if you want to allow anonymous users to have access to this Portal.

12. Click **Next**.

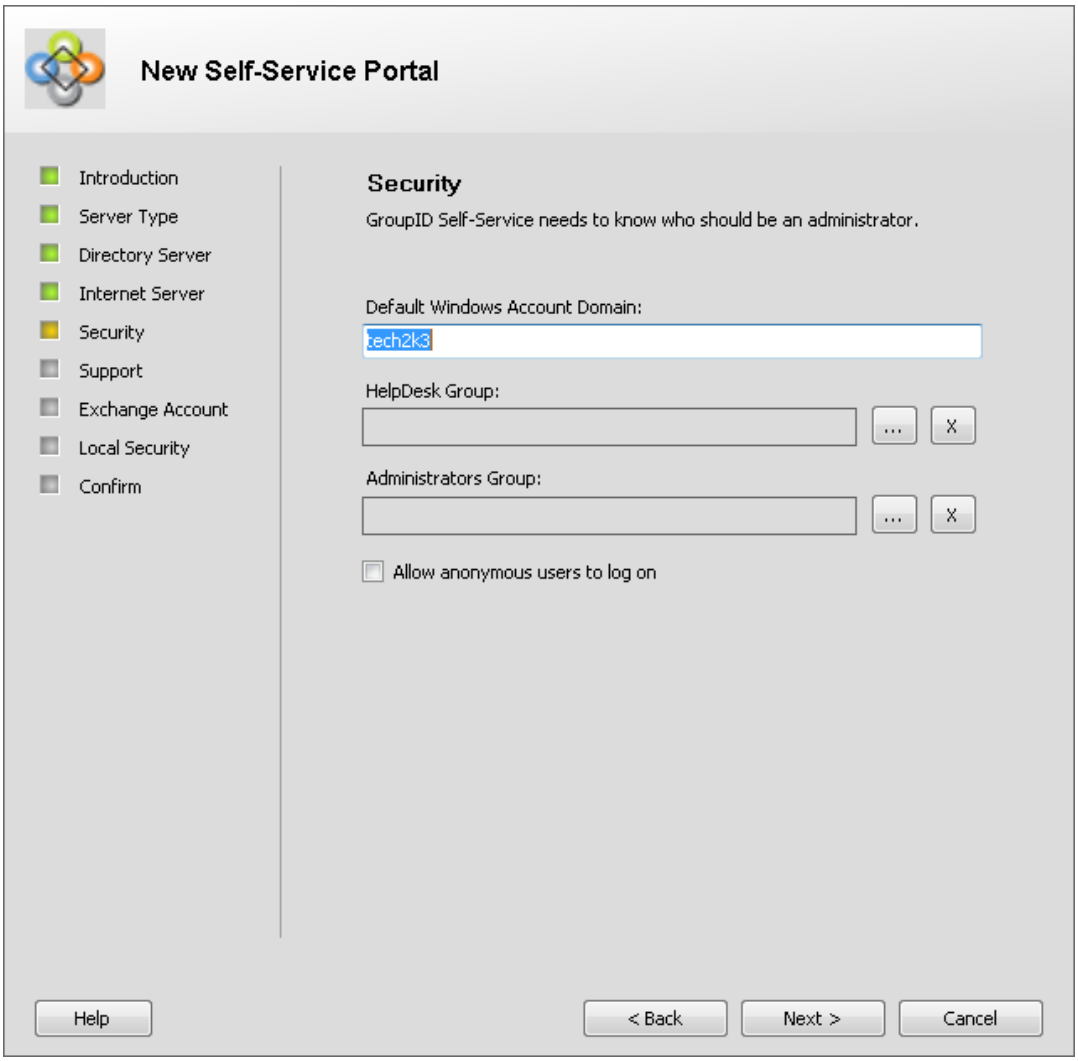


Figure - The Security page

13. The **Support Information** page, by default, shows the support and contact settings defined on the GroupID **Configurations** dialog box. However, you can change these settings for the Portals individually. To do this:

    i. In the **Support group/administrator's e-mail address** box, type the e-mail address for the group or contact that will be responsible for providing support for this Portal.

    ii. In the **Help URL** box, you can type the Internet address for a Web page or Web site to locate your custom help files.

14. Click **Next**.

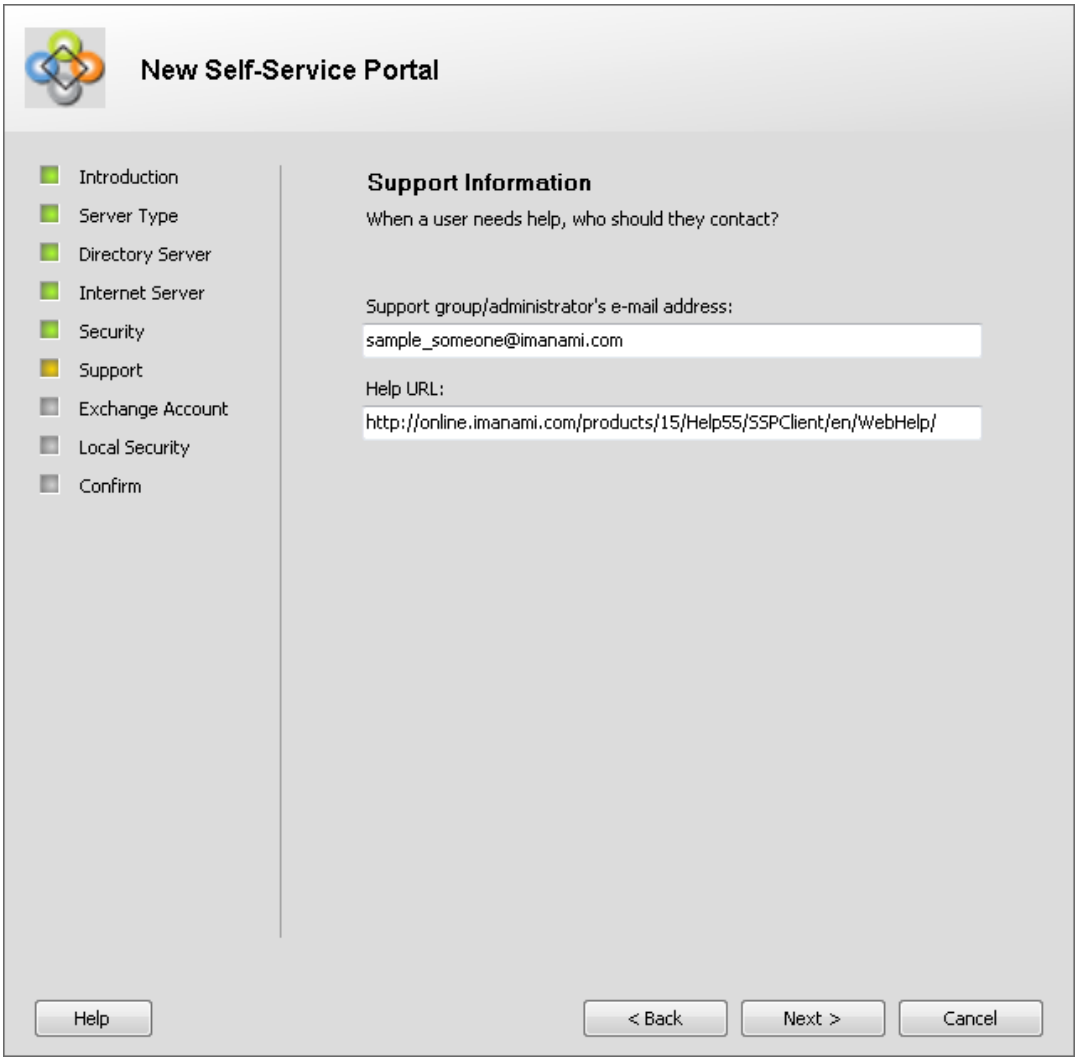


Figure - The Support Information page

15. The next two pages of the wizard: **Exchange Account** and **Local Policy** are for informational purposes only. Click the **Next** button after reviewing the information on these pages to continue.

16. The **Confirm** page shows the information that you have entered in the previous pages. Verify the information on this page. If you need to change anything, click **Back** until you reach the required page.

17. After reviewing the information, click **Finish**. This step completes the Portal setup. The Portal will now be prepared and once its ready it will appear in the **Portals** node of GroupID Management Console. The Portal can now be accessed using a Web browser.

Duplicate a Portal

Self-Service Portal will let you duplicate the default configuration of an existing Portal. Duplicating a Portal copies only the server configurations of the Portal.

To create a duplicate Portal, please follow the instructions provided below:

1. If not already open, launch GroupID Management Console.
2. Under the **Self-Service Portals** node, right-click the Portal you want to copy and click **Copy Portal**. GroupID displays the **GroupID-Self Service Portal** dialog box.
3. In the **Server name** box, type a unique name of the Portal and click **OK**.
   This will start the wizard for creating a new Portal.
4. GroupID displays a dialog box for you to enter the name of your Portal. Type a unique name for the Portal and click **OK**.
   This will start the **New Self-Service Portal** wizard.
5. By default, the wizard pages contain the default settings of the copied Portal which you can update for the new Portal by following the same steps as given in the section **Create a new Portal** earlier in this chapter.

Setting Functionality Mode

You can use functionality modes to restrict the functionality of the Self-Service Portal for enterprise users. For more information about the functionality modes, see **Self-Service Functionality Modes** in **Chapter 3, Introduction**.

You can set the required functionality mode by following the instruction provided below:

1. Launch the GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node and then expand the required Portal.
3. Click the **Server** node and then click the **Functionality** tab.
4. From the functionality modes list, click the required mode.
5. On the toolbar, click **Save** .

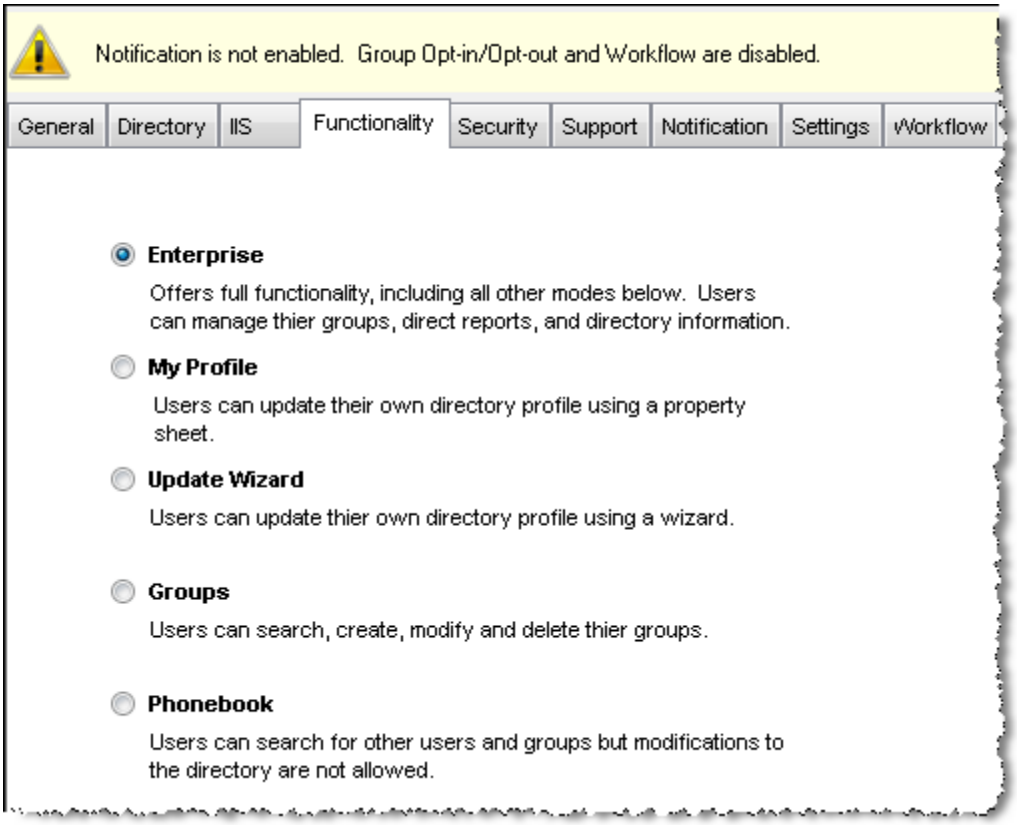

Notification is not enabled. Group Opt-in/Opt-out and Workflow are disabled.
General
Directory
IIS
Functionality
Security
Support
Notification
Settings
Workflow
Enterprise
Offers full functionality, including all other modes below. Users can manage thier groups, direct reports, and directory information.
My Profile
Users can update their own directory profile using a property sheet.
Update Wizard
Users can update thier own directory profile using a wizard.
Groups
Users can search, create, modify and delete thier groups.
Phonebook
Users can search for other users and groups but modifications to the directory are not allowed.

Figure - The Functionality tab

Chapter 5: Portal Configuration

This section provides information on controlling the overall configurations of the Portal. The configurations are divided into the following sections:

Directory Settings, contains information on how to connect Self-Service Portal to an Active Directory domain.

Web Server Settings, explains the process of setting IIS and default language for the Portal.

Security Settings, provides information on how Self-Service determines the privileges of the users logging on to the Portal.

Support Contact Settings, describes how you can modify the contact information for your internal support and the address of the online help.

Notification, explains how to configure SMTP server for sending e-mail notifications for the changes made to the directory through the Portal.

Advance Settings, describes how to add customization to the Portal using advance settings.

Directory Settings

While creating a Portal, you specify the Active Directory domain the Portal will connect to along with the account credentials that the Portal will use for communicating with the domain. You can change these Portal settings any time you require. You can connect the Portal to a different domain and provide the account credentials for communication.

> It is recommended that the account should have **Enterprise Admin** and **Domain Admin** permissions on the Active Directory.

Keep in mind that an Active Directory domain controller only has authority to change objects in its domain or forest. Therefore, the Portal can only modify objects in the Active Directory domain or forest in which the specified server resides.

To change the directory settings, please follow the instruction given below:

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node.
3. Expand the node for the required Portal and click the **Server** node.
4. Click the **Directory** tab.
    i. In the **DNS Domain Name** box, type the name of the Active Directory domain you want to connect to.
    ii. In the **User name** box, type the domain name and user name, separated by a backslash (\), of the account the Portal should use to connect to the domain.
    iii. In the **Password** box, type the password for the specified user account.
    iv. On the toolbar, click **Save** .

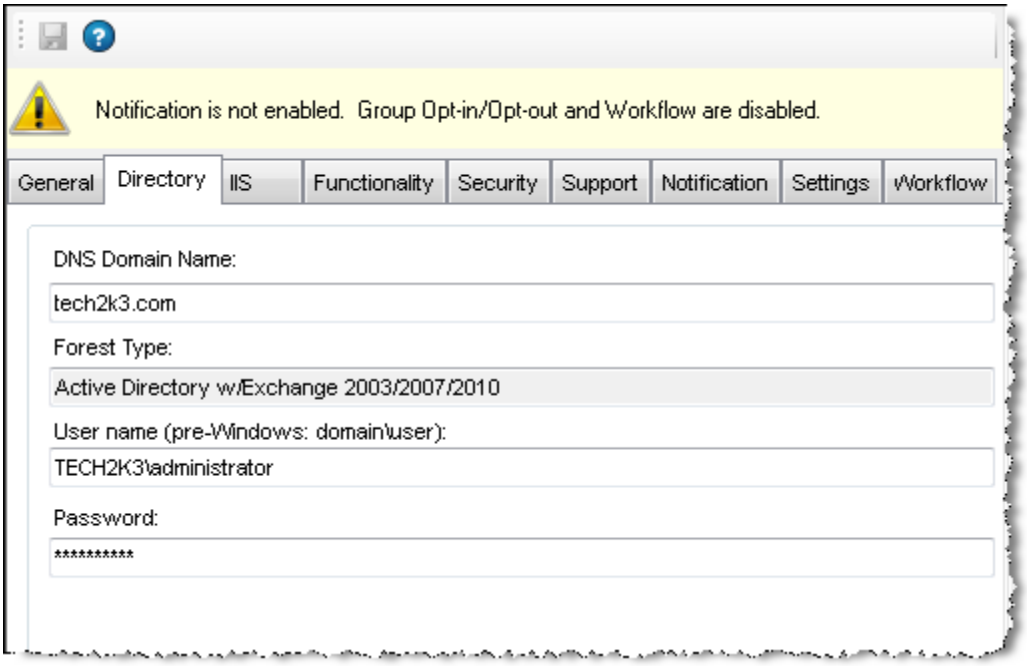


Figure - The Directory tab

Web Server Settings

Self-Service Portal runs within a virtual directory on the Internet Information Server (IIS). When you create the Portal, Self-Service copies files required to run the Portal into the template directory of the local file system path to create a virtual directory on the Web server (IIS). You can change the Web server for the Portal, if required.

You can also specify the default language for the Web browser of the user. Self-Service Portal detects the languages supported by the Web browser program of the user when they log on and attempts to load the interface with the correct language. If it does not support the language set for a user's browser, or it cannot detect the language settings of the Web browser, it will load the default language of English.

To manage the Web server settings, please follow the instructions given below:

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node.
3. Expand the node for the required Portal and click the **Server** node.
4. Click the **IIS** tab.

To change Web server

- From the **IIS Server** list, select the required server. The default selection is, **Default Web Site**.
- On the toolbar, click **Save** .

To change the default language

- From the **Select default locality** list, click the required language.

- On the toolbar, click **Save** .

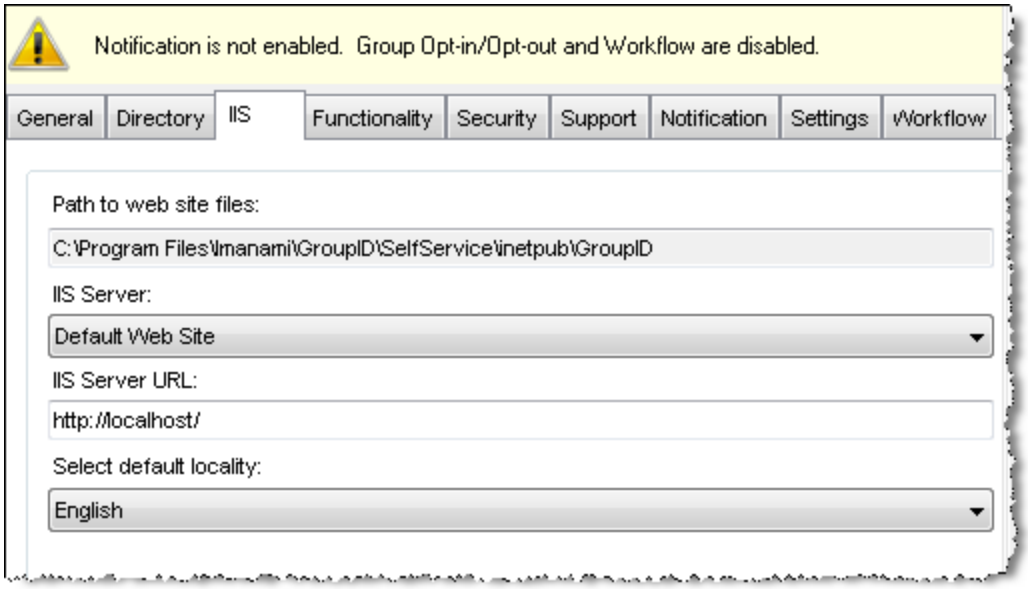


Figure - The IIS tab

Security Settings

Authentication of users visiting a Self-Service Portal is carried out by IIS on which the Portal is deployed. The types of authentication methods that you can configure for your Portal depends on the version of IIS installed on your server. IIS 6.0 supports eight authentication methods.

1. Anonymous authentication
2. Basic authentication
3. Digest authentication
4. Advanced Digest authentication
5. Integrated Windows authentication
6. UNC authentication
7. .NET Passport authentication
8. Certificate authentication

For more information about IIS authentication types, please refer to the Microsoft TechNet Web site - http://www.microsoft.com/technet.

Security Groups

Self-Service has its own mechanism of identifying the privileges of users logging on to a Portal. Self-Service divides the Portal users into four groups: **Administrators**, **Helpdesk, Normal Users** and **Anonymous Users**. When a user logs on to a Portal, Self-Service checks to see the group the user belongs to in order to determine their privileges.

The administrators group and helpdesk group can be used in a cross forest domain. This is based on the forest trust level provided.

	Group	Description
1	Administrators	Users belonging to this group have complete control over the Portal. They can perform all activities that the Portal interface supports.
2	Helpdesk	This group is a level below administrator, but has more administrative privileges than a normal and anonymous user. Users belonging to this group can modify Active Directory objects but they cannot create new mailbox, user or custom recipient. There is an advance setting that allows the helpdesk user to create a new mailbox, user or custom recipient. For more information, see **Advance Settings** later in this chapter.
3	Normal Users	All other users (not belonging to the administrator or helpdesk group) are considered as **Normal Users** and they can manage their own directory information.
4	Anonymous Users	These users can use the Portal as a **Phone Book** without logging on to the Portal. They can search the directory but cannot modify any of its attributes.

To manage security groups, follow the instructions given below:

1. Launch GroupID Management Console.
2. Expand the **Self-Service** node, and then expand **Portals**.
3. Expand the node for the required portal and click the **Server** node.
4. Click the **Security** tab.

To add Helpdesk Group

1. Click button next to the **Helpdesk Group** box.
   i. On the **Select Recipients** dialog box, enter the name of the group that you want to set as the Helpdesk group.
   If your entered name results in multiple matches, a **Multiple Names Found** dialog box will be displayed for you to select the correct item.
   ii. Click **OK**.
2. On the toolbar, click **Save** .

To add Administrators Group

- Follow the same steps as given for setting the **Helpdesk Group**.

To Allow anonymous access

1. Select the **Allow anonymous users to log on** check box.

2. On the toolbar, click **Save** .

Specifying security groups is optional. You can skip these, if you do not want anyone to have these permissions within the Portal.

Figure - The Security tab

Support and Logging Settings

Portals have a **Contact** and **Help** link in their user interface. The former is for sending an e-mail to the administrator or helpdesk for inquiries or support while the latter opens up the online help for the portal in a new browser window. Both these links are customizable and their target e-mail address or Web address can be set using the instructions given later in this section.

Figure - Help and Contact links in the Web Portal.

Also available with the contact and help link settings are the log settings. The log settings here are specific to the portal under consideration and will take precedence over the global log settings. The global log settings apply to the whole Self-Service module and are used as the default settings for new portals. The global log settings can be set from the GroupID Configurations dialog box.

Logging can be used for tracking events that might help in tracing out the cause of a problem. Usually they are used for debugging errors. Log settings and their configurations for Self-Service are explained in the topic **Log Settings** in **Part 7: GroupID Configurations.**

To manage these setting, follow the instructions given below:

1. Launch GroupID Management Console.
2. Expand the **Self-Service** node, and then expand the **Portals** node.
3. Expand the required Portal and click the **Server** node.

4. Click the **Support** tab.
   The tab, by default, shows the support contact, help and logging settings defined on the GroupID **Configurations** dialog box. These settings are explained in detail in the topic **Log Settings** in **Part : GroupID Configurations**. You can customize these settings individually for each portal.

To add the e-mail address of the support contact

The e-mail address can be of a user, contact or group. This will be mapped to the Contact link on the portal.

1. In the **Support group/administrator's e-mail address** box, type the e-mail address of the support contact.

2. On the toolbar, click **Save** .

To add a Web site address

The default URL set here points to Imanami's online help for Self-Service portals and is mapped to the Help link on the portal. You can change this to point to your own version of the help, an internal helpdesk Web site, or similar.

1. In the **Help URL** box, type the Web site address.

2. On the toolbar, click **Save** .

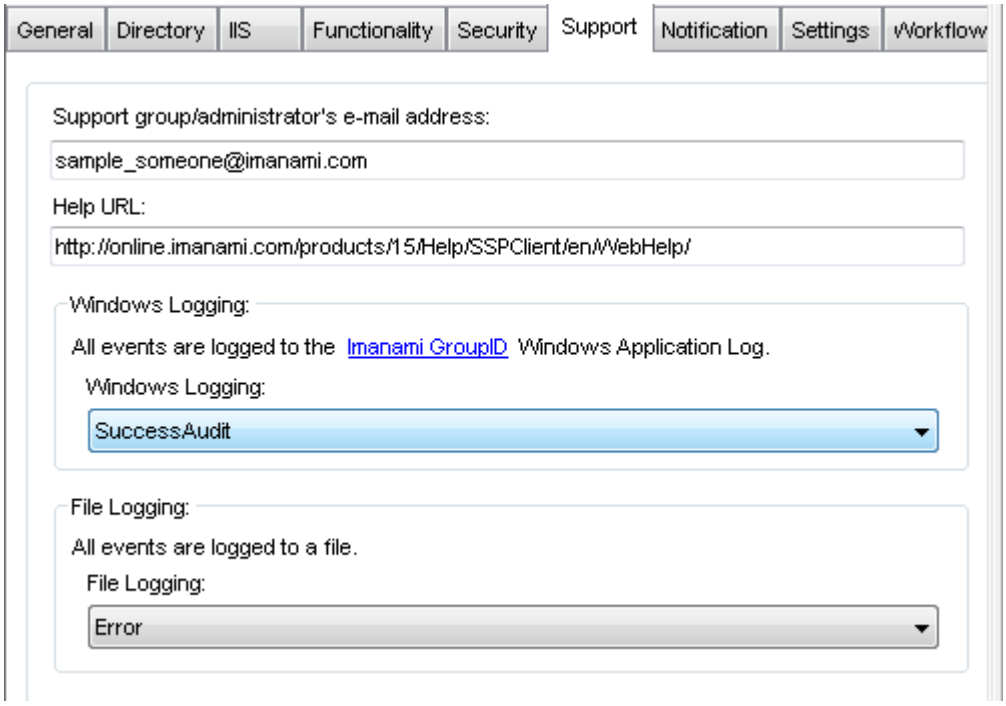


Figure - The Support tab.

Notification Settings

A Self-Service Portal can send e-mail notifications about the changes users make to the directory using it. Notifications combined with Workflows enable you to implement control and monitor user activities. For information on Workflows, see **Chapter 6: Workflows**. You need to configure a SMTP server for sending e-mail notifications.

The steps below guide you on how to configure the SMTP server:

1. Launch GroupID Management Console.
2. Expand the **Self-Service** node, and then expand **Portals**.
3. Expand the required Portal node and then click the **Server** node.
4. Click the **Notification** tab.
    i. In the **Notification method** list, click **SMTP**. This enables the fields in the **SMTP Server Options** area.
    ii. In the **Server name/IP address box**, type the IP address or DNS name of the SMTP server to use for sending notifications. This server must allow relaying.
    iii. In the **Port** box, type the SMTP port to use when connecting. The default port is 25.
    iv. In the **From e-mail address** box, type the e-mail address to use as the sending address for notifications.
    v. In the **To e-mail address** box, type the recipient e-mail address or addresses (separated by semicolon (;)).
    vi. In the **CC e-mail address** box, type the e-mail address or addresses (separated by semicolon (;)) of the recipients who should receive a copy, if required.
    vii. You can select the **Notify Owner/Manager** check box to have the primary owner, additional owners or manager of a modified object notified along with the recipients specified in the **To** e-mail address.
    viii. On the toolbar, click **Save** .

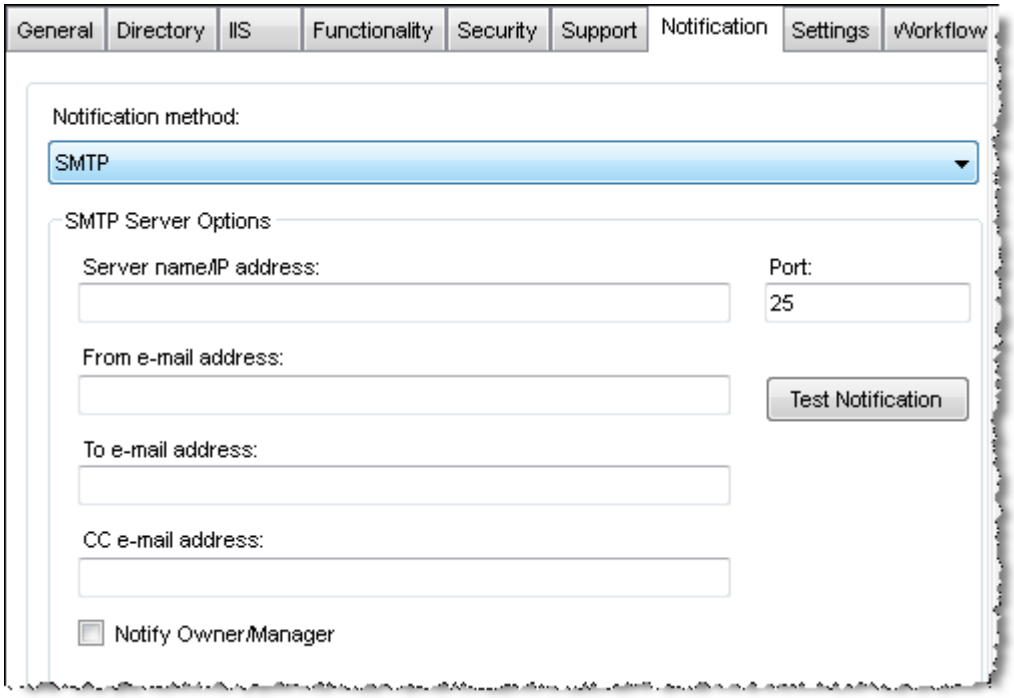


Figure - The Notification tab

Advance Settings

Self-Service supports advance settings to the Portal that can add customization to the functionality and appearance of the Portal. For example, you can add a setting to show the employee's photo when someone visits their profile (for more information, see **Add Photo to User Profile** in **Chapter 7: Customizing the Portal**) or you can add a setting to restrict administrators from deleting groups and so on. Some settings are available in all user interfaces of the Portal while others are specific to a particular user interface.

To add advance settings, please follow the instructions given below:

1. Launch GroupID Management Console.
2. Expand the **Self-Service** node, and then expand **Portals**.
3. Expand the required Portal and click the **Server** node.
4. Click the **Settings** tab.
    i. Click **Add**.
    ii. On the **Add Setting** dialog box:
        a. In the **Key** box, type or select the required setting.
        b. In the **Value** box, type the setting value.
        c. Click **OK** to close the dialog box.

iii. On the toolbar, click **Save** .

You can edit a setting by selecting it from the list on the **Settings** tab and clicking **Edit**. A setting can be deleted by clicking **Remove**.

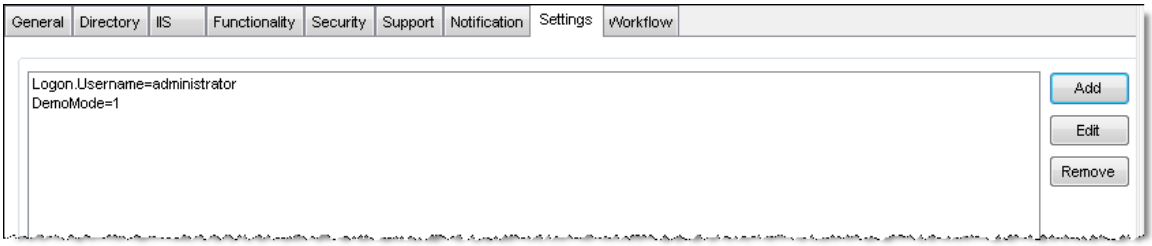


Figure - The Settings tab

Below is the list of all available settings that you can use to fine-tune your Portal implementation.

Setting	Value	Description
DefaultStartPage	Page Name	Sets the default start page for all authenticated users. Choose from search.aspx, groups.aspx, mygroups.aspx, mydirectreports.aspx, mymemberships.aspx, and default.aspx. The default is default.aspx that is the welcome page. Note that some Functionality Modes do not support some start page values.
DemoMode	1/True or 0/False	When set to 1 (or True), it disables the change and reset password features. The default is 0.
Editobj.DefaultMemberLimit	100	Number of items to show, by default, on the Members tab and Delivery Restrictions tab (Accept from and Reject from lists) of the Group Properties. The default value is 100.
Editobj.PictureURLField	Field Name	Field Self-Service should examine for user pictures. Default is "url".
Engine.LogonContainer	Container path	Allows only users within the specified container to log on.
Engine.LogonSuperFilter	LDAP criteria/filter	Allows only recipients that match the specified criteria.
Engine.NotifyEndUser	1/True or 0/False	When set to 1 (or True), it sends an e-mail notification of changes to the user making the change. The default is 0.

Setting	Value	Description
Engine.NotifyObject	1/True or 0/False	When set to 1 (or True), it sends an e-mail notification to the object (user or contact) being modified. The default is 0.
Engine.NotifyWithCustomTemplates		No longer supported in GroupID 6.0.
Engine.ReadOnly	1/True or 0/False	When set to 1 (or Ture), it prevents Self-Service from actually updating the directory. Notification still occurs. The default value is 0.
Engine.SearchContainer	Container path	Returns search results that match the specified criteria and that are in the specified container. If Search.SearchDefault setting is also defined, then this setting is ignored and objects are searched according to the value set for Search.SearchDefault.
Engine.SearchSuperFilter	LDAP criteria/filter	Returns only the search results that match the specified criteria and this criteria.
Groups.AllowOwnerDelete	1/True or 0/False	When set to 0 (False) the user will not be able to delete groups. The Delete action item is removed unless the user is a member of the admin group or the help desk group.
Group.RestrictBulkImport	1/True or 0/False	When set to 1 (True), the bulk import functionality will be restricted for group owners.
Logon.Username	Username	Forces Self-Service to authenticate every user as this user. This is helpful for demonstration only.
Logon.WWW-Authenticate	BASIC or NEGOTIATE	Used to allow MAC running IE 5.X to authenticate. Default is NEGOTIATE.
NewObject.Container	Container path	If specified, Self-Service will not prompt non-

Setting	Value	Description
		administrative users for the container of a new object.
NewObject.GroupTypeScope	SecurityDomain / SecurityGlobal / SecurityUniversal / DistributionDomain / DistributionGlobal / DistributionUniversal	Groups Only: Specify the group type and scope. If specified, Self-Service will not prompt the user for the information when creating a new group.
NewObject.ObjectType	UserME / UserMBE / Contact / Group	Type of object to create. If specified, Self-Service will not prompt for the object type to create. UserME is for mail-enabled user creation and UserMBE is for mailbox enabled user creation.
NewObject.RootContainer	Distinguished name of the domain or container	Sets the domains and containers that will be available to user for creating new objects using a Self-Service Portal. When set, the user will only be able to create objects in the specified domain/container and its sub-domains/sub-containers (if any). Use semi-colon(;) as separator when specifying more than one domains or containers. Example: DC=Imanami,DC=US; OU=HR,DC=Imanami,DC=PK; OU=Sales,DC=Imanami,DC=PK
Picture.FilePath		Identifies the path to the images.
Picture.Attribute		Identifies the attribute that should match the picture name.
Picture.Suffix		Identifies the extension of the picture file.
Search.DefaultPageSize	10	Sets the default page size for displaying search results. The user can override this setting.

Setting	Value	Description
		Default value is 10.
Search.UseContainsFilter	1/True or 0/False	Controls whether the search page uses a "starts with" filter or "contains" filter. "Starts with" filters provide better performance. Default is 0, which uses the "starts with" filter.
Search.Sort	Field name	Field name to sort the search results by. Default is to sort by displayName. Set this setting to nothing to disable sorting.
Search.DisplayAdditonalGroupsInMyDeletedGroups	1/True or 0/False	Controls whether to show the groups for which the logged on user is set as additional owner in the "My Deleted Groups" view. Default is 0.
Search.DisplayAdditonalGroupsInMyExpiredGroups	1/True or 0/False	Controls whether to show the groups for which the logged on user is set as additional owner in the "My Expired Groups" view. Default is 0.
Search.DisplayAdditonalGroupsInMyExpiringGroups	1/True or 0/False	Controls whether to show the groups for which the logged on user is set as additional owner in the "My Expiring Groups" view. Default is 0.
Search.DisplayAdditonalGroupsInMyGroups	1/True or 0/False	Controls whether to show the groups for which the logged on user is set as additional owner in the "My Groups" view. Default is 0.
Search.SearchDefault	GlobalCatalog or domain	Sets the selection in the "Search" list available on the toolbar of some pages and all Search pages. Setting its value to GlocalCatalog selects the "Entire Directory" check box in the Search list, by default and changing its value to Domain selects the logged on domain.
Toolbar.DefaultMRUCount	5	Number of Most Recently Used objects to display in

Setting	Value	Description
		toolbar. The default is 5.
Toolbar.SearchGCForReportsGroups	1/True or 0/False	Controls whether the Global Catalog or local domain are searched when a user clicks the "My Groups" and "My Direct Reports" buttons. Default is 1.
Toolbar.ShowPhoneList		No longer supported in GroupID 6.0. If this setting was being used in GroupID 5.0; then while upgrading the Portal to 6.0, the access level of this setting will automatically be set to 999 which means that the Phone List will be available to all users.
Toolbar.ShowNewGroup	1/True or 0/False	Determines whether to show the New Group toolbar item to non-Administrators. Default is 1.
Toolbar.HideChangepassword		No longer supported in GroupID 6.0. If this setting was being used in GroupID 5.0; then while upgrading the Portal to 6.0, the access level of this setting will automatically be set according to its value in GroupID 5.0.
Toolbar.HideMembersClearButton	1/True or 0/False	When set to 1 (or True), it removes the Clear button that shows on the Members tab of the New Group wizard. The Clear button removes all users from the members list without having to select them individually. The default is 0.
Toolbar.HideHelpLink	1/True or 0/False	When set to 1 (or True), it removes the Help link from the top navigation bar. The default is 0.
Toolbar.HideResetPassword		No longer supported in GroupID 6.0. If this setting was being used in GroupID 5.0; then while upgrading the Portal to 6.0, the access level

Setting	Value	Description
		of this setting will automatically be set according to its value in GroupID 5.0.
UnlockAccounts	1/True or 0/False	When set to 1 (or True), it causes Self-Service to reset locked out accounts when the password is reset. The default is 0.

Chapter 6: Workflows

This chapter provides comprehensive information about workflows. Instructions on setting-up workflows and managing the workflow requests are also included in this chapter.

The chapter is divided into the following sections:

Overview, gives an overview of workflows and explains how they add an additional layer of administration to your Active Directory data.

System Workflows, explains System workflows and provides their set up instructions.

User-defined Workflows, explains User-defined workflows and provides their set up instructions.

Configuring Notifications, describes how you set-up SMTP server for sending e-mail notifications.

Managing Workflow, describes how you can view, approve, deny and re-route workflow requests.

Overview

Self-Service has a built-in auditing system to ensure that correct data is entered by users before applying changes in Active Directory. The data integrity is ensured by implementing workflows.

A workflow defines a set of rules that you can apply to specific object fields in the Portal. This set contains settings that answer the following questions:

1. On which objects to apply the workflow?
2. On which event should the workflow trigger?
3. The fields that should be present for the object to trigger the workflow
4. The fields to monitor
5. Who the request should be sent to for approval?

When an action is carried out on the Portal by user, it is evaluated according to these settings before affecting the Active Directory. If no approval is required, the change takes place immediately. If approvers are set for the workflow then an approval must be gained, it automatically routes the request to the approving authorities for the necessary approval. Once the approval is received and approved, the Portal automatically makes the requested changes in Active Directory and notifies the requester and approvers (except the one who has approved the request) by an e-mail (if SMTP server is configured for the Portal). If approval is denied, it does not update the information within Active Directory and a notification is sent to the requester and the approvers (except the one who has approved the request) with an explanation of why it was denied (requires SMTP server to be configured).

Workflows add additional layer of administration by letting you supervise only the user activities of interest on the Portal. You define workflows for all critical fields and let GroupID do the rest. Whenever there will be a change in any of your specified fields by the end users, the relevant workflow will be automatically triggered and you will receive a notification about the changes. The changes will not take place until approved by you.

Self-Service divides workflows into two categories:

- System workflows
- User-defined workflows

Workflow Events

A workflow event defines the action that when takes place causes the workflow to be triggered. Self-Service divides the workflow events into three categories: **Create**, **Edit** and **Delete**. When any one of these events occurs for an object (Group, User or Contact), it is first evaluated according to the workflow route defined for it, and then changes take place in the Active Directory.

The table below describes how the occurrence of these events for Active Directory objects cause the workflows to be triggered.

Event	Object	How the workflow triggers?	Approver
Create	Group	User requests to create a new group. You can define only one workflow	• Owner of the group (includes

Event	Object	How the workflow triggers?	Approver
		route for the Create event of the Group object.	primary and additional owners) • Any person or group
	User	User requests to create a new mail-enabled or mailbox-enabled user. You can define only one workflow route for the Create event of the User object.	• Any person or group
	Contact	User requests to create a new contact. You can define only one workflow route for the Create event of the Contact object.	• Any person or group
Edit	Group	User requests to change a field value for the designated group that requires an approval.	• Owner of the group (includes primary and additional owners) • Any person or group
	User	User requests to change a field value for the designated user that requires an approval.	• Manager of the user • Any person or group
	Contact	User requests to change a field value for the designated contact that requires an approval.	• Manager of the contact • Any person or group
Delete	Group	User requests to expire the designated group.	• Owner of the group (includes primary and additional owners) • Any person or group
	User	User requests to delete the designated user	• Manager of

Event	Object	How the workflow triggers?	Approver
		(mail-enabled or mailbox-enabled).	the user • Any person or group
	Contact	User requests to delete the designated contact.	• Manager of the contact • Any person or group

System Workflows

Self-Service provides four system workflows which are triggered automatically when their relevant actions take place:

1. **Require Admin Approval to change Group Expiration Policy** - this workflow is triggered when a user changes the expiration policy of a group. By default, this workflow is disabled and no approver is assigned to it.
2. **Workflow to Nest a Group** - this workflow is triggered when security groups (semi-private, semi-public and public) are added into the membership of other groups. By default, group owner (includes primary and additional owners) is selected as the workflow approver.
3. **Workflow to Join a Group** - this workflow is triggered when a user joins a semi-private group. By default, group owner (includes primary and additional owners) is selected as the workflow approver.
4. **Workflow to Leave a Group** - this workflow is triggered when a user leaves a semi-private group. By default, group owner (includes primary and additional owners) is selected as the workflow approver.

The rules for these workflows are pre-defined, but Self-Service allows you to customize their approvers if required. When a new Portal is created, these workflows are by default set as enabled (except **Require Admin Approval to change Group Expiration Policy** workflow). However, you can disable them any time by simply clearing the **Enabled** check box for the required workflow on the **Workflow** tab.

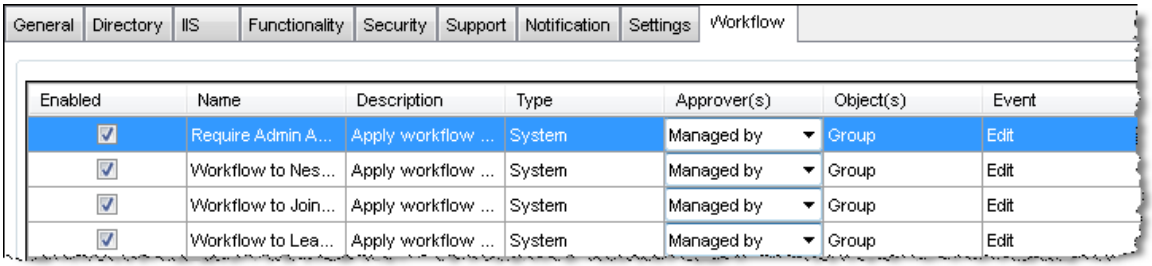


Figure - System Workflows

User-defined Workflow

A user-defined workflow is the one that is set up by yourself according to your requirement. You have complete control over the objects and events on which the workflow applies, conditions to trigger the workflow, fields to be included in the workflow request and the approvers for approving the requests.

Setting up a User-defined Workflow

> User-defined workflows require notifications to be enabled. For information on enabling notifications, see **Configuring Notification** later in this chapter.

The instructions below describe the procedure for defining a workflow route to prevent users - with a manager - from changing their **Department** and **Assistant** until approved by their manager.

1. Under the **Self-Service** node, expand the **Portals** node.
2. Expand the required Portal and then click the **Server** node.
3. Click the **Workflow** tab.
4. Click **Add**. This displays the **Workflow Route** dialog box. On the dialog box, you will need to provide the following information:
    i. In the **Name** box, type a name of the workflow.
    ii. In the **Description** box, type a brief description of the workflow.

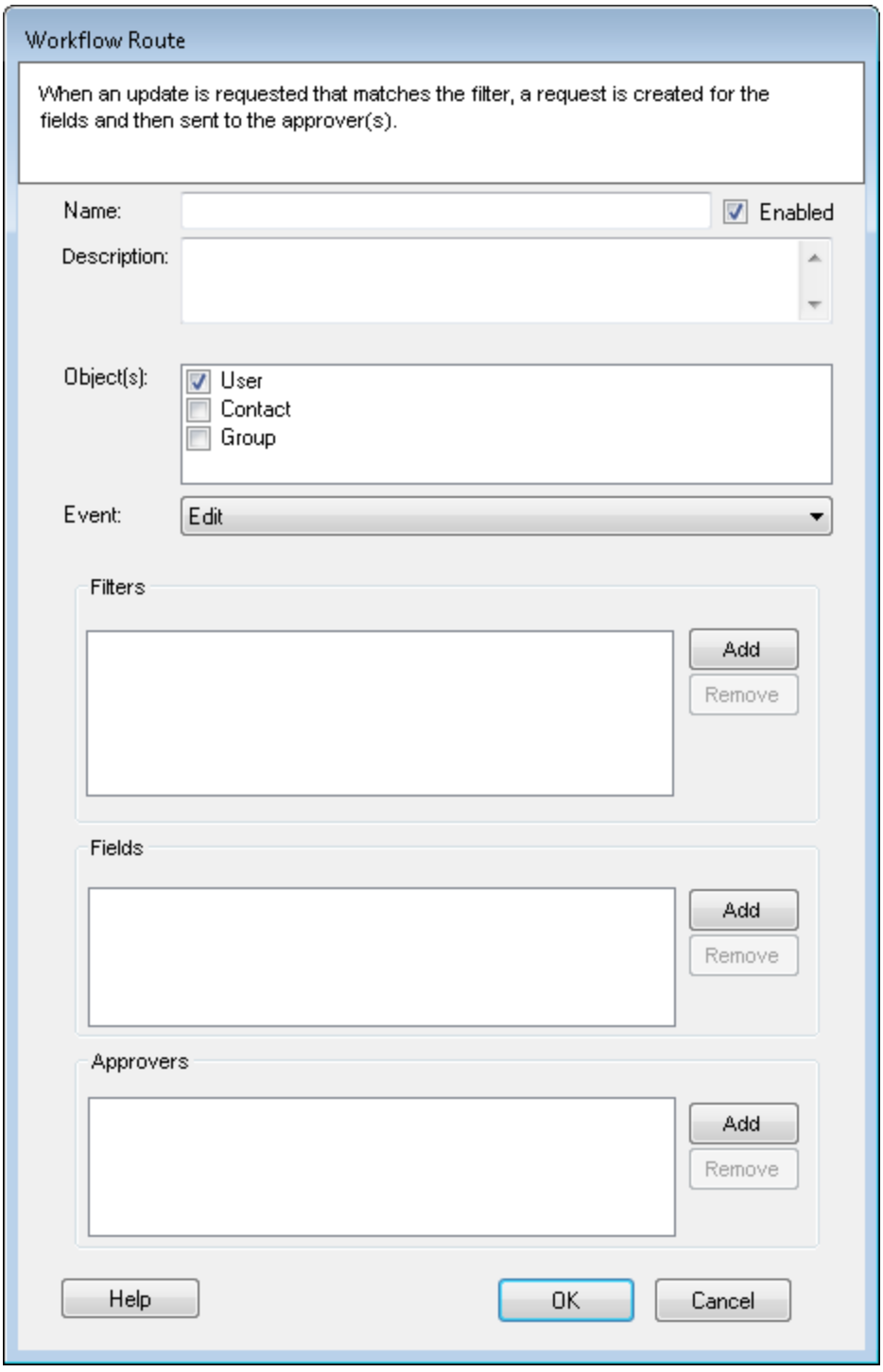


Figure - The Workflow Route dialog box

iii. Next, select the objects on which you want to apply the workflow. In this scenario, the User is the required object, so in the **Object(s)** list, select the **User** check box. If you want to apply the workflow on other objects as well i.e. Contact and Group, select their respective check boxes. Otherwise clear them (if selected).

iv. Next, select the event that when performed on the object will trigger the workflow. For this scenario, select **Edit** from the **Event** list.

v. Next, add filters for the workflow route. Filters determine conditions that a change must satisfy in order to trigger a workflow. For this scenario, users with a manager is the condition to trigger the workflow. To add this filter:

- In the **Filters** area, click **Add**. This displays the **Add Filter** dialog box, where:

  a. In the **Field** list, click **manager**. This list contains all Active Directory and Exchange (if installed on the server you are connected to) attributes.

  b. In the **Condition** list, click **is present** which implies that the **manger** attribute should be present for the workflow to be triggered.

  c. The **Value** box is not available for the **is present** and **is not present** conditions because these operators are not comparison operators. They only check if the value for the selected field exists or not and depending upon that return either true or false. In the **Value** box, type the value (not case-sensitive) that determines whether the condition satisfies the requirement for this route.

  d. Click **OK** to close the dialog box.

Filters and **Fields** are not available for the **Create** event.

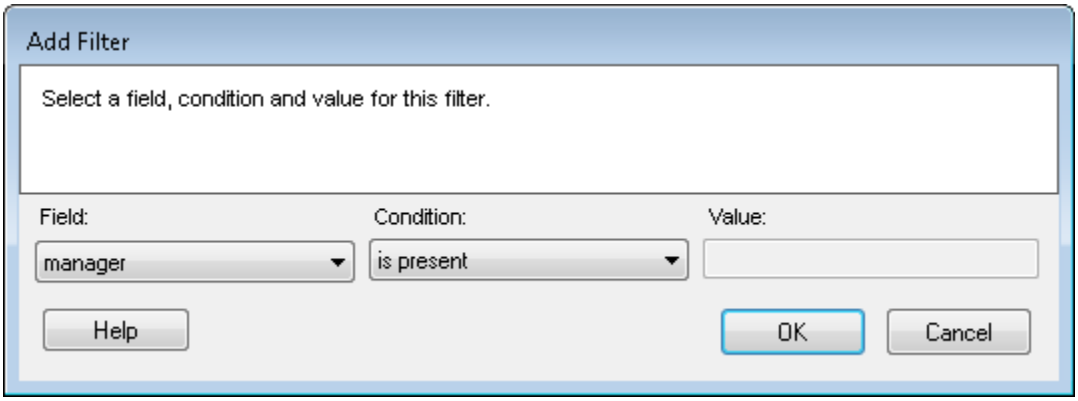


Figure - The Add Filter dialog box

vi. Next, add fields that require approval when changed. For this scenario, **Department** and **Assistant** are the required fields. To add these fields:

a. In the **Fields** area, click **Add**. This displays the **Add Field** dialog box, where:

- In the given list, click **department**.
- Click **OK** to close the dialog box.

b. Repeat the step 7(vi)(a) to add the **assistant** field.

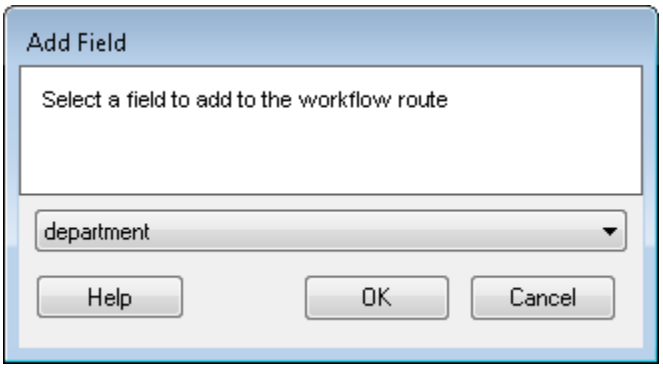


Figure - The Add Field dialog box

vii. Next, add approvers who are to approve or deny a change for the given fields. When an approver approves the request, a change is made in the directory immediately and the approvers (except the one who has approved the request) are notified about the change. When an approver denies a change request, an e-mail is sent back to the requester and the approvers (except the one who is denying the request) with an explanation for the denial. For this scenario, **Manager of User** is the approving authority. To set it:

- In the **Approvers** area, click **Add**. This will display the **Add Approver** dialog box, where:

  a. Click **Manager of User**. This will examine the **manager** attribute of the user, when changes are made to the **department** or **assistant** fields; and will route the approval request to them. The **Add Approver** dialog box shows two more options depending on the objects and event selected. These are:

  - **Owner of Group**, select this to set the primary and additional owners (including Exchange 2010 additional owners for Exchange 2010 environments) of the group as approvers for any changes made to the specified fields. In case of a change, the request will be routed to all owners for approval. If the group does not have any owner or additional owners, no request will be generated and an error will be displayed to the user.

  - **This person**, select this to specify the user or group that you would like to set as the approver. Click the **Select** button to select the user.

  b. Click **OK** to close the dialog box.

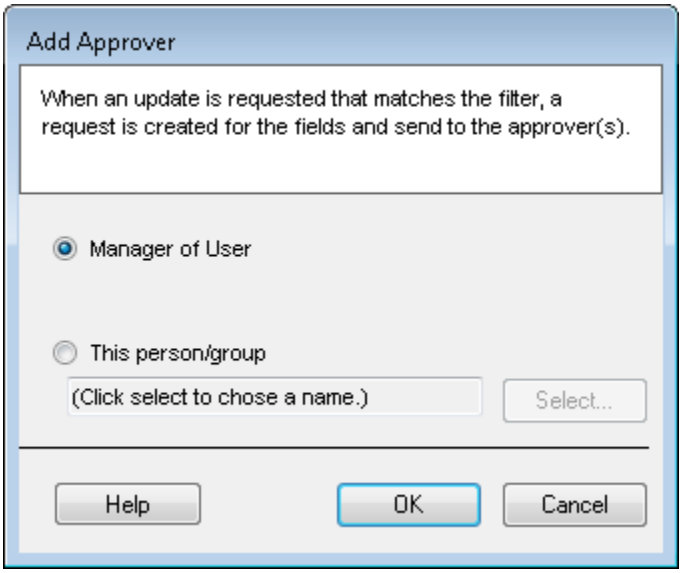

Add Approver
When an update is requested that matches the filter, a request is created for the fields and send to the approver(s).
Manager of User
This person/group
(Click select to chose a name.)
Select...
Help
OK
Cancel

Figure - The Add Approver dialog box

viii. Click **OK** to close the **Workflow Route** dialog box.

5. On the toolbar, click **Save** .

Configuring Notification

Before setting up workflows, first make sure that SMTP (Simple Mail Transfer Protocol) server is properly configured and tested for sending e-mail notifications to the approvers when changes are made to the Portal.

For information about configuring the SMTP server, see **Notification** in **Chapter 5: Portal**.

Managing Workflow Requests

You can view all workflow requests that are either generated by you or enterprise users by expanding **Self-Service** node in the tree view of GroupID Management Console. The workflow requests are categorized into two main nodes:

1. **All Requests**, contains all workflow requests that have been generated by enterprise users through different Self-Service Portals created on your machine. The list includes both pending and processed requests.

2. **My Requests**, contains workflow requests that have been generated by you from different Self-Service Portals created on your machine. The list includes both pending and processed requests.

Clicking any of the request nodes will show the list of relevant requests with the detailed information about the request which includes request generator, status, creation date, portal ID and so on. You can expand a request to view the list of fields to be approved along with their current and proposed values.

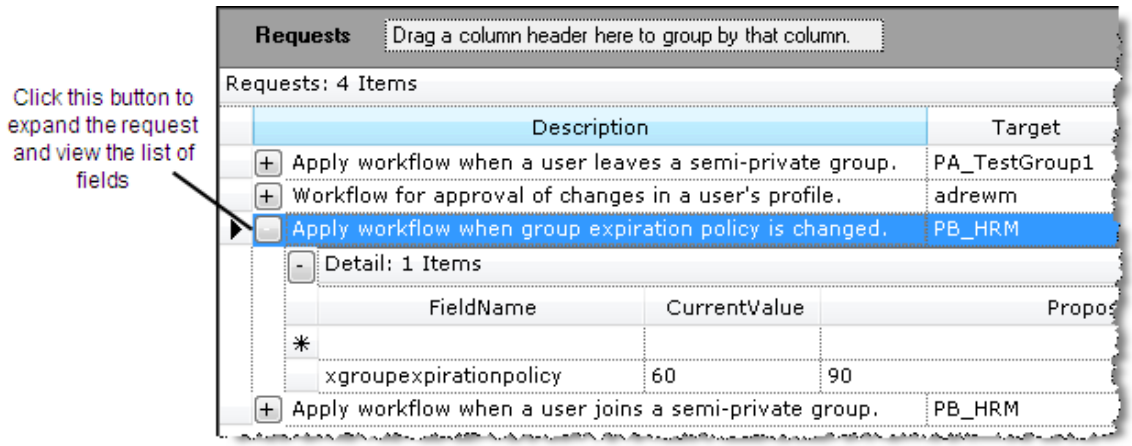


Figure - Requests list showing a request in expanded format

The information on managing workflow requests is provided in the following sections:

- Approve a Request
- Deny
- Re-route Request to another Approver
- Re-route Request to multiple Approvers

Approve a Request

After viewing the details for a pending request, if you are satisfied with the changes proposed by the end user, you can approve the request by following the instructions below:

1. Expand the **Self-Service** node.

2. Next, click the **All Requests** node.

3. From the **Requests** list, right-click the request to approve and then click **Approve**.

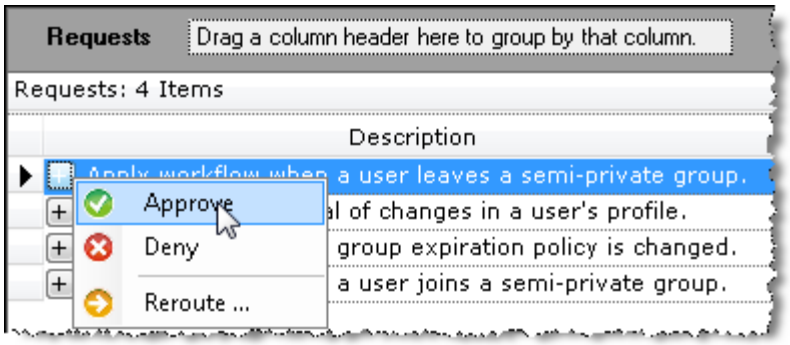


Figure - The Approve command on the shortcut menu

Deny a Request

If you are not satisfied with the changes by the end user, you can simply deny the request by following the instructions below:

1. Expand the **Self-Service** node.
2. Next, click the **All Requests** node.
3. From the **Requests** list, right-click the required request and then click **Deny**. This displays a dialog box asking you to enter the denial reason.
4. In the **Denial Reason** box, type the reason of request denial and click **OK**.

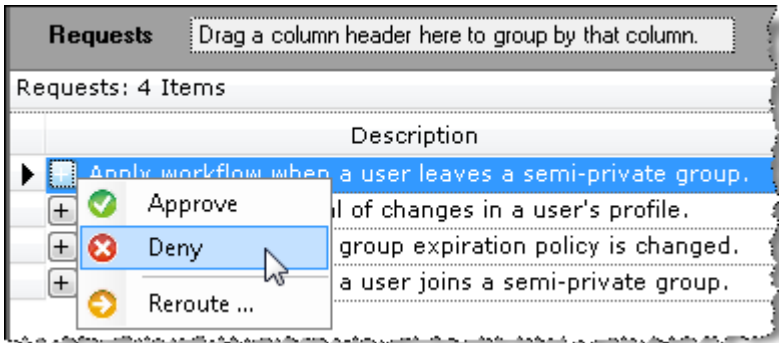


Figure - The Deny command on the shortcut menu

Re-route Request to another Approver

An administrator can manage workflow requests for all users. If an approver is out of office and many workflow requests are pending in their account, the administrator can re-route the requests to other appropriate approvers and get them resolved quickly. When the request is re-routed, a notification e-mail is also sent the new approvers notifying them about the routed request.

For re-routing request to other approvers:

1. Expand the **Self-Service** node.
2. Next, click the **All Requests** node.
3. From the **Requests** list, right-click the request to re-route and then click **Reroute**.

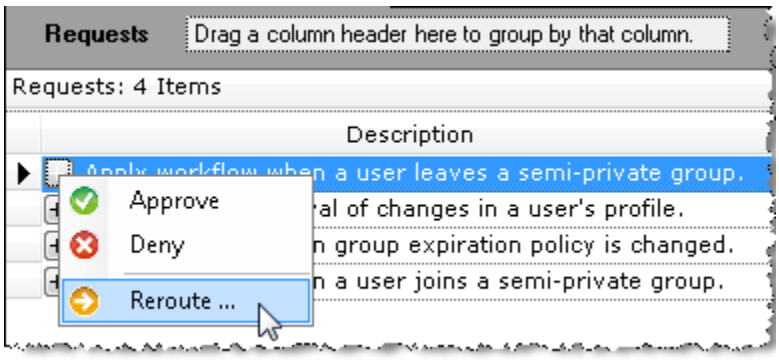


Figure - The Reroute command on the shortcut menu

This displays the **Select Approver(s)** dialog box showing the approver of the workflow for which the request was generated.

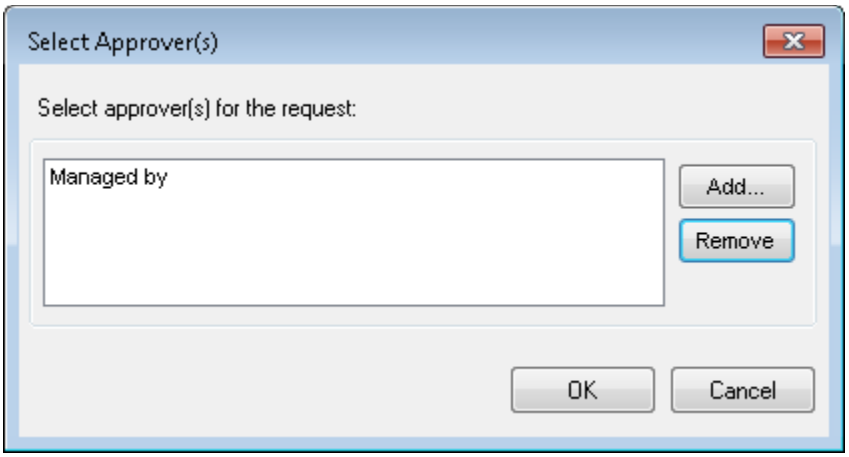


Figure - The Select Approver(s) dialog box

4. On the **Select Approver(s)** dialog box:

    i. Click **Remove** to remove the existing approver.

    ii. Click **Add** to display the **Add Approver** dialog box to select the required approver.

Re-route Request to multiple Approvers

Administrators can entitle multiple users as acting approvers of workflow requests in absence of the primary approver and can re-route requests to all of them.

The procedure for re-routing requests to multiple approvers is same as provided in the previous section except that you can add as many approvers as required using the **Add Approver** dialog box.

Chapter 7: Customizing the Portal

Self-Service allows administrators to customize different elements of a Portal depending on the requirements and privileges of enterprise users. This chapter provides information on how administrators can control the layout and appearance of Web pages depending on user privileges.

The chapter is divided into following sections:

Add Photo to User Profile, shows how you can add visual identifications to the users profile.

Display Types, explains how you can use display types to control the pattern of data, users can enter for different fields of the Portal.

Customize Search Form, provides information on how you can control the fields to be displayed on search forms and search results of the Portal.

Customize Update Wizard, contains steps for customizing pages and fields of the update wizard.

Customize My Properties, explains how you can control the properties of directory objects for displaying on the Portal.

Navigation Bar, describes customizations of the left Navigation bar of the Portals.

Bad Words, explains how users can be restricted from entering offending words while using the Portal.

Rename Active Directory, explains how you can assign descriptive and meaningful names for complex Active Directory attributes for the import/export members and additional owners feature.

Add Photo to User Profile

Self-Service Portal users have the option to set photo for their profile that helps in visually identifying them when someone visits their profile. In this regard, the **Home Page** field on the user properties page is designated where the user can provide the Web address of their profile picture. This picture is displayed on the **General** tab when the user profile is launched.

There are also some settings available on the GroupID Management Console using which administrators can add photos to users' profile. The photos added by administrators take precedence over the photos set by users through the Web Portal.

The example below shows how you can add photo to a user's profile using the GroupID Management Console. Note that these steps are to be performed on the same computer where the Portal is created.

1. Create a new folder on your computer and save the user photo to that folder. The file should be named as ***Display Name of the User*.jpg**.
2. Now, launch the GroupID Management Console and expand the **Self-Service** node.
3. Next, under the **Portals** node, expand the required Portal.
4. Click the **Server** node and then click the **Settings** tab.
5. Click the **Add** button.
6. On the **Add Setting** dialog box:
    i. In the **Key** box, type or select **Picture.FilePath**.
    ii. In the **Value** box, type the location of the folder where the photo is saved. For this example, the user's photo is saved at the location **C:\SSP\ProfilePhotos**.
    iii. Click **OK**.
7. Repeat steps 5 and 6 to also add the following settings:
    - **Key:** Picture.Attribute, **Value:** DisplayName
    - **Key:** Picture.Suffix, **Value:** .jpg

You can provide any attribute for the **Picture.Attribute** setting and any extension for the **Picture.Suffix** setting but the files for the user photos should also be named accordingly.

8. On the toolbar, click **Save** .

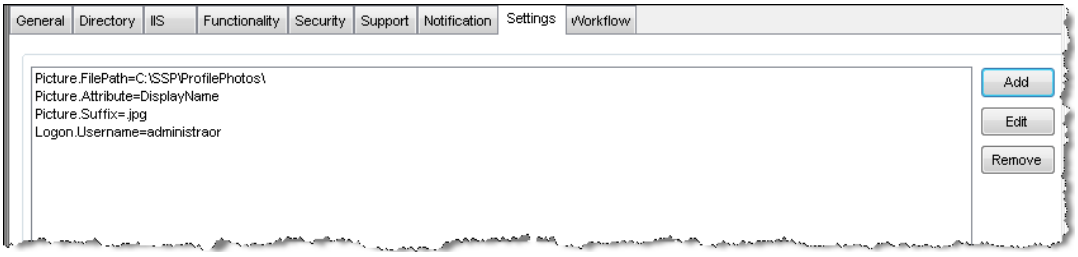


Figure - The Settings tab showing settings for users photos

9. Launch the Portal, open the user profile and you will see the photo appearing on the **General** tab.

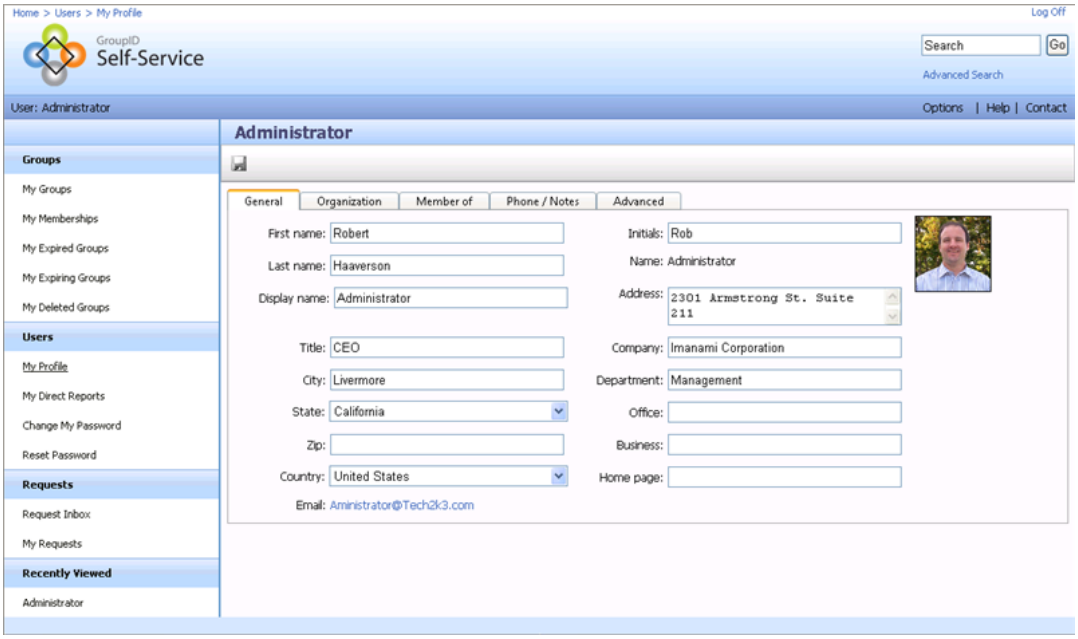


Figure - The profile page showing the user's photo

Display Types

Self-Service Portal offers an intuitive front-end to network users for interacting with Active Directory attributes. Each Active Directory attribute can contain value of certain type. Some can contain single string value (examples; name, sAMAccountName) while others can have multiple values (example; proxyAddress). Some can only accept distinguished names (one or more) (examples; members, memberOf) while others allow only Boolean values, True or False (examples; hideDLMembership, isDeleted).

To ensure that the portal users update these attributes in the same manner as it is supported by Active Directory, Self-Service introduces the concept of Display types. A Display type controls what user interface element should be used for presenting an Active Directory attribute on the portal and on what format the user can enter data for it. Display types provide an on-screen validation check for the data entered by users before actually saving changes to the directory.

Self-Service display types cover almost all types of Active Directory attributes (Single-valued, multi-valued, boolean, distinguished name and so on). However, based on their characteristics and customization options, these display types are divided into two categories:

- Basic Types
- Custom Types

Basic Types

Self-Service divides display types into eight basic categories Text box, drop-down list, linked field drop-down list, password, check box, multi-value, DN and DNs. Almost all Active Directory attributes somehow fit in any of these types. Some of these basic types can be linked with Active Directory attributes straight away while others require customizations before applying on any attribute. These customizations are explained in detail in the topic Custom Types.

Below is a brief explanation of each basic display type along with its association with Active Directory attributes:

Text box

Text box type is for collecting and displaying a single value. This type can directly be linked with an Active Directory attribute. However, if you want to apply some additional rules on it, for example; you want to assign a default value or apply some validation rules on the data entered, you can make a custom type using this basic type. Validation rules for the data entered in the text box can be enforced by implementing regular expressions. Regular expressions ensure that the entered data is according to the required format.

Drop-down list

Drop-down list type is used where you want to provide users the list of possible options from which they have to select one. Self-Service does not allow you to directly use this type. You have to create a custom type for it where you set the values that will be shown in the list and a default value for it. This custom type can then be linked with an Active Directory attribute.

Linked field drop-down list

Linked field drop-down list type is used to isolate a user's choice to one key field. When the key field is entered, it will auto-populate the linked fields with their appropriate values. For example, when a user selects the office he works in; the business telephone number and fax number are auto-populated, as well. Self-Service does not allow you to use this type directly. You have to create a custom type using this basic type where you define the key value, linked fields and their values. This custom type can then be linked with an Active Directory attribute, entering the key value for which will populate other fields.

Password

Password type can be used for the Active Directory attributes containing confidential information. The user interface element on which the Password type is applied appears as a text box on the portal. However, the text appearing in the box is replaced with bullets or asterisks.

Check box

Check type is used for those Active Directory attributes that can only accept true or false values. reportToOwner, reportToOriginator, oOFReplyToOriginator are some of the attributes that accept true/false value. This type requires no customizations so can be linked with an Active Directory attribute straight away.

Multi-value

Mutli-value type is used for those Active Directory attributes that can accept multiple string values. By default, none of the pre-defined user interface element of the portal (the elements that are available when the portal is created) is presented with this type. However, you can add a new user interface element or modify existing one for multi-valued Active Directory attribute of this type. For example, you can change the type of **Business 2** UI element (available on the **Phone/Notes** tab of the **User** properties) to multi-value. The user interface elements having their type set to multi-value appear on the portal as shown in the following figure:

Figure - Showing the multi-value type applied on the Business 2 field

Clicking the icon shows a dialog box where you can add new values and remove existing ones. No customizations are required for this type so it can directly be linked with an Active Directory attribute.

DN

This type is used for the Active Directory attributes accepting distinguished name as their value. Assistant, altRecipient are some of the attributes that accept distinguished name. The user interface element on which the DN type is applied, appears as a button on the portal pages clicking which shows the **Search** dialog box where you can add or remove the desired object. DN type can directly be linked with an Active Directory attribute since no customizations are required for it.

DNs

DNs type is used for those Active Directory attributes that can accept multiple distinguished names. For example, member, memeberOf. The user interface element on which the DNs type is applied, appears like:

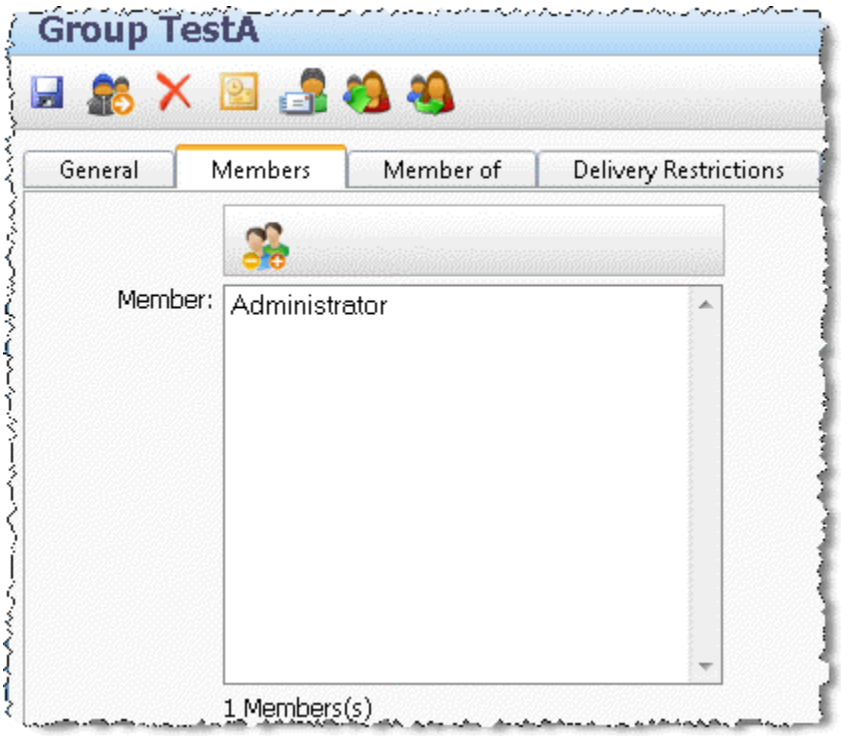


Figure - DNs type is applied on Member filed

Clicking the icon shows the **Search** dialog box where you can add or remove the desired objects. No customizations are required for this type so it can directly be linked with an Active Directory attribute.

Custom Types

As explained earlier, Self-Service supports customizing the basic display types. The customization can be as simple as specifying a default value for an element or can be as complex as linking multiple elements on the basis of values and binding relationships available in an XML file.

Based on the customization levels Self-Service offers for basic data types, custom types are divided into two categories:

1. Simple Types
2. Linked Combo

Simple Types

Simple types are derived from three basic types: text box, drop-down list and linked field drop-down list, with additional customizations applied on it. For example, you can define a simple text box type for telephone number and apply a validation rule on it that it can only accept phone numbers in US format, or you can define a simple drop-down list type containing the list of departments in your organization, or you can create a simple linked field drop-down list type where selecting the office number populates its phone number and fax number. Simple types once defined can be linked to as many fields as required. Self-Service provides few pre-defined simple types out-of-the-box that are available by default when the portal is created. However, you can add more simple types according to your business requirements.

Adding a text box simple type

A text box type has the following properties:

- **Name**, a unique name.
- **Default value**, the value that will appear in the text box, by default.
- **Regular Expression**, a regular expression is a pattern of text that consists of ordinary characters (for example, letters a through z) and special characters, known as metacharacters. Regular expressions ensure that the entered data is according to the required format. For example, the regular expression for US Phone Number (pattern: (555) 123-4567) will be: ^\(\d\d\d\) \d\d\d-\d\d\d\d.

When you create a new portal, few text box types are already available with it that you can use to link to any field. The properties of these text box types are set to the following values:

	Name	Default Value	Regular Expression	Regular Expression Example
1.	maskPhoneUSwithExt	None	^\(\d\d\d\) \d\d\d-\d\d\d\d x\d\d\d$	(555) 123-4567 x890
2.	SmtpEmail	None	^([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*@([0-9a-zA-Z][-\w]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,9})$	someone@imanami.com
3.	maskPhoneUS	None	^\(\d\d\d\) \d\d\d-\d\d\d\d$	(555) 123-4567
4.	maskEmailAddress	None	^([a-zA-Z0-9_\-\.]+)@((\[[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.)|(([a-zA-Z0-9\-]+\.)+))([a-zA-Z]{2,4}|[0-9]{1,3})(\]?)$	user@domain.com
5.	maskZipCode	None	\d{6}(-\d{4})?	NNNNNN-NNNN

You can define more text box types, if required. The instructions below guide you through the process of adding a new text box type for validating social security number according to US format:

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node.
3. Expand the required Portal node and click the **Design** node.
4. Click the **Custom Display Types** tab.
5. Click **Add**. This displays the **New Display Type** dialog box. On the dialog box:

i. In the **Name** box, type a unique name for the display type. Choose a name that is descriptive and helps you easily recognize it. You cannot modify the name once you have created the text box type.

ii. From the **Type** list, select **Textbox** and then click **OK**.

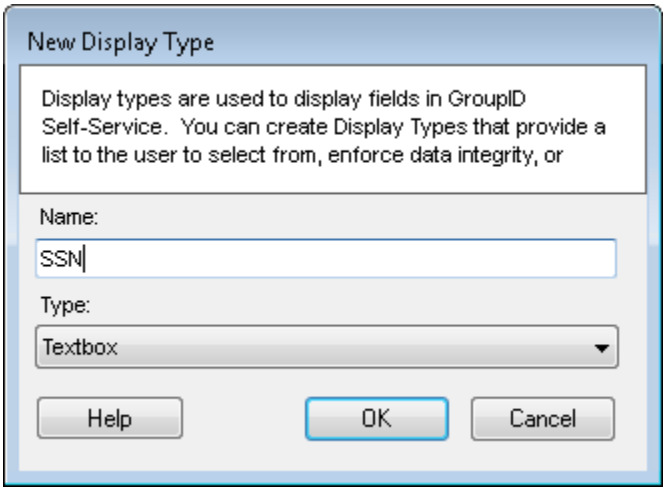

New Display Type
Display types are used to display fields in GroupID Self-Service. You can create Display Types that provide a list to the user to select from, enforce data integrity, or
Name:
SSN
Type:
Textbox
Help
OK
Cancel

Figure - The New Display Type dialog box

iii. On the **Edit Design Type** dialog box, type the information for the given fields:

a. In the **Default value** box, type a default value that you want to display in the text box. For this scenario, leave it blank.

b. In the **Regular Expression** box, type the regular expression to validate data entered into the text box. For SSN validation, type the expression **^\d{3}-\d{2}-\d{4}$**. You can leave this box blank if you do not want to apply any validation rule on the data entered.

c. In the **Regular Expression Example** box, you can provide an example to show the valid format of data that should be entered in the text box. For SSN example, you can type **111-22-3333**.

d. Click **OK** to close the **Edit Design Type** dialog box.

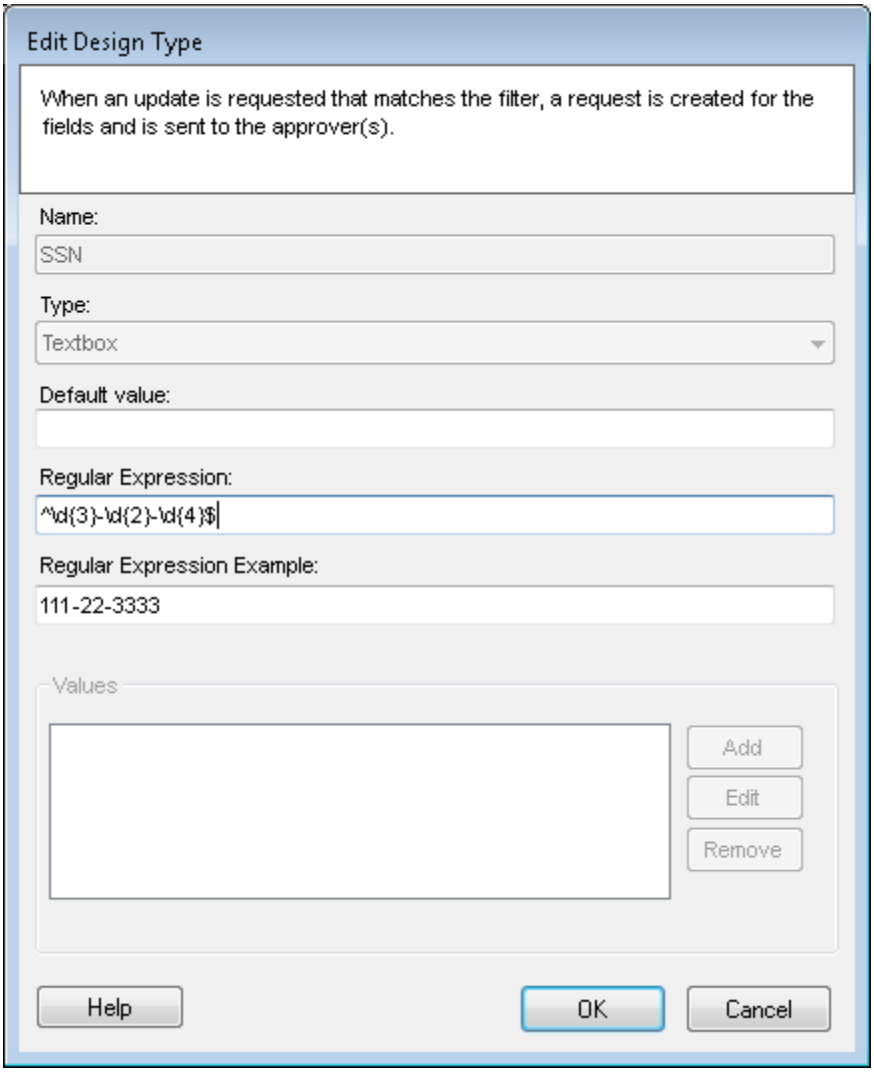


Figure-The Edit Design Type dialog box while adding a new text box display type

This text box type can now be linked to the fields defined for taking **SSN**.

Adding Drop-down list type

A drop-down list display type has the following properties:

- **Name**, a unique name.
- **Default Value**, the value that will be selected by default in the list.
- **Values**, the list of all values that will appear in the drop-down list.

When you create a new portal, few drop-down list types are already available with it that you can use to link to any field. The properties of these types are set to the following values:

	Name	Default Value	Values
1.	lstCountry	None	*The list all countries.*

	Name	Default Value	Values
2.	lstState	None	*The list of all states in US.*
3.	lstStateProvince	None	*The list of all states and provinces in US.*
4.	lstProvince	None	*The list of all provinces in US.*
5.	linkedState	None	None

You can define as many drop-down list types as required. The instructions below guide you through the process of adding a new drop-down list type for showing the list of all departments in your organization. The procedure of adding a drop-down list type is quite similar to adding a text box type. Only few steps differ which are stated as follows:

1. On the **Display Type** dialog box, select **Dropdown List** from the **Type** list.
2. On the **Edit Design Type** dialog box:
    - The **Values** area becomes available where you can add, edit or remove values in the drop-down list.
    - The Default value should be picked from the list of values added in the drop-down list.
3. Click **Add** in the **Values** area. This displays another dialog box where you can type the value for the drop-down list.

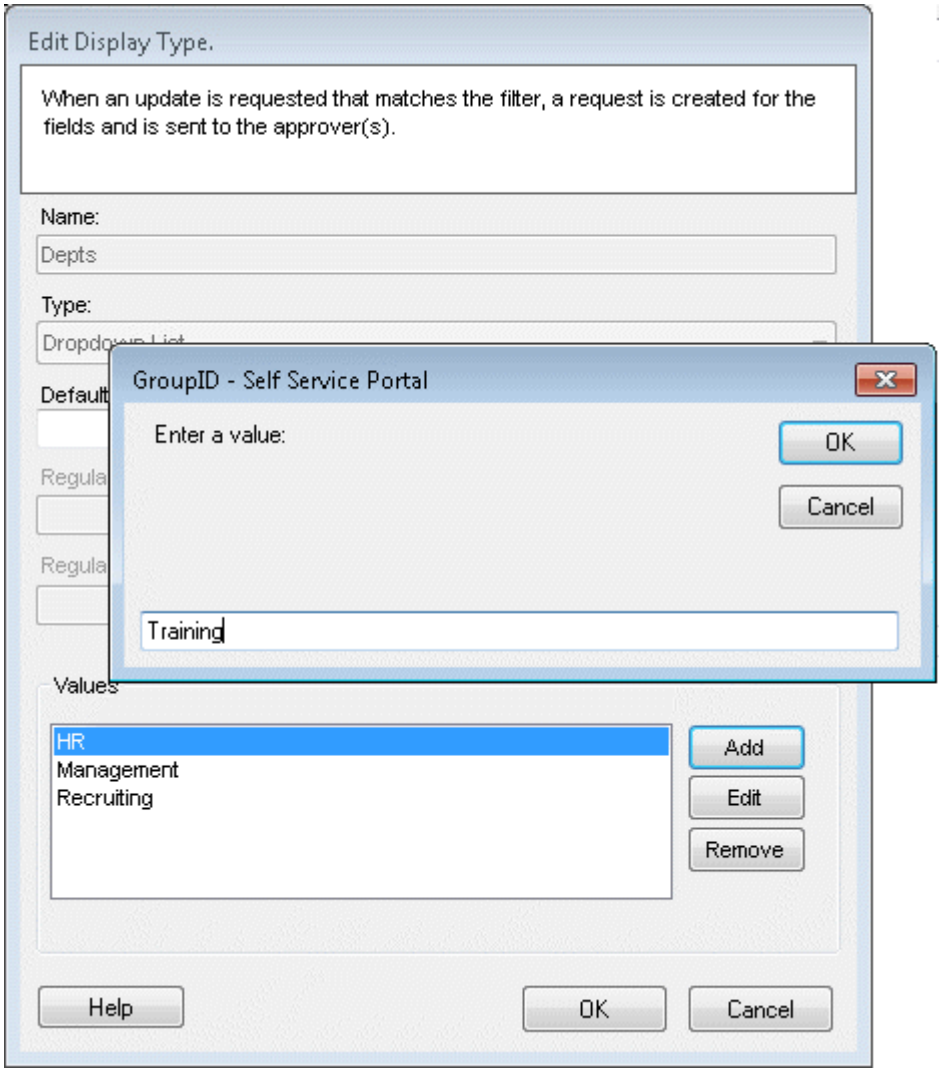


Figure - The dialog box for adding value in the drop-down list

This drop-down list type is now ready to be linked to the **department** attribute.

Adding a Linked Field Drop-down list type

A linked field drop-down list has the following properties:

- **Name**, a unique name.
- **Key Value**, the value that when selected in the drop-down list populates the linked fields.
- **Linked Field**, the fields that will be linked with the key field.
- **Value,** the values of the linked fields.

With the creation of a new portal, by default, no linked field drop-down list is available. However, you can create new linked field drop-down list types, if required. The instructions below explain the procedure for creating a new linked field drop-down list for populating **Business Phone Number** and **Fax Number** fields as the **Office Number** is entered. The steps for adding a new linked field drop-down list type are similar to those for adding a drop-down list display type with the following few differences:

1. On the **Display Type** dialog box, select **Linked Field Dropdown List** from the **Type** list.

2. On the **Edit Design Type** dialog box, click **Add** in the **Values** area. This displays the **Edit Linked Field Values** dialog box, where:

    i. In the **Key value** box, type the key value. For this scenario, we want to enter the business phone number and fax number for Office Number **306**, so type **306** in this box.

    ii. In the **Linked Fields** area, click **Add**. This displays the **Edit Linked Field Value** dialog box, where:

        a. In the **Field** box, type or select the **telephonenumber**.

        b. In the **Value** box, type the business phone number.

        c. Click **OK**.

iii. Follow the step 2(ii) for adding the following:

        a. **Field**: fascimileTelephoneNumber

        b. **Value**: *office Fax number*

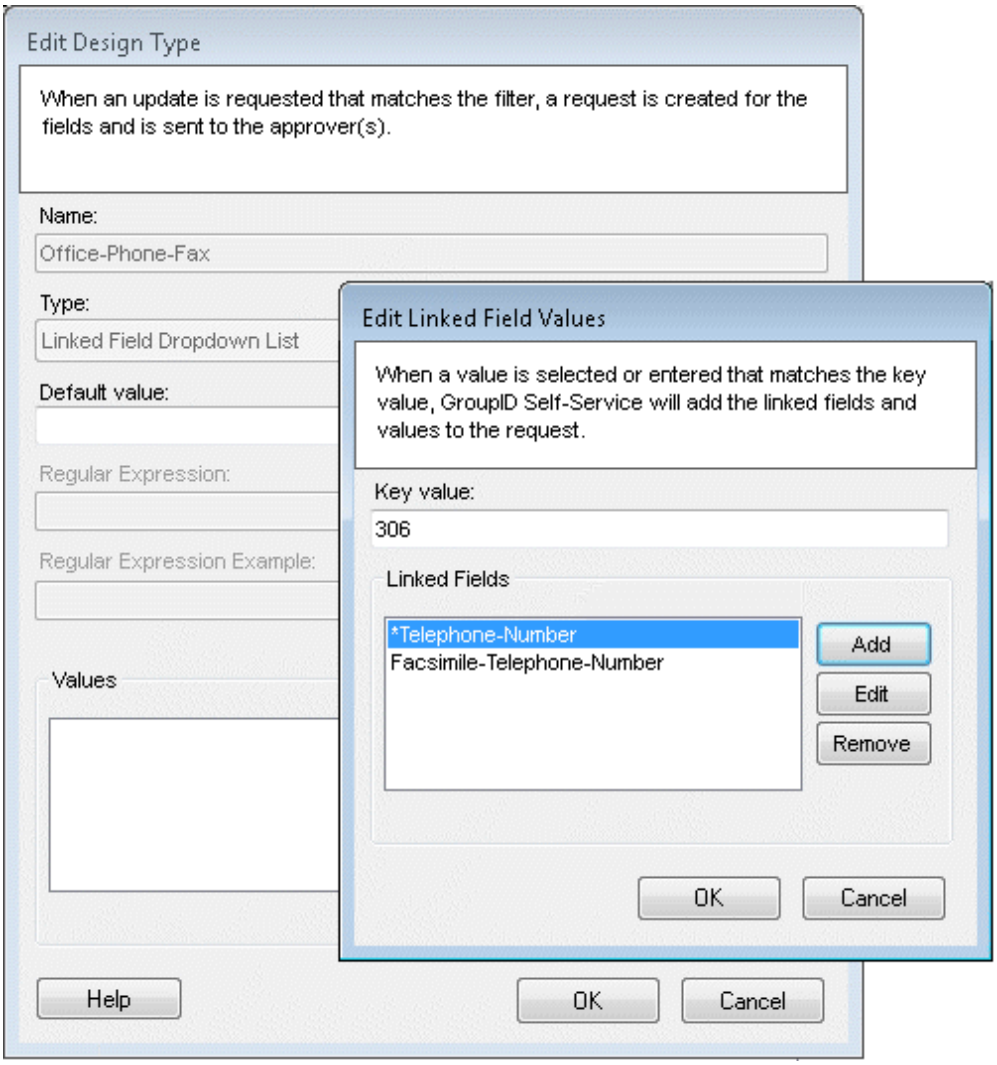


Figure - The Linked Field Values dialog box showing the added linked fields

This new linked field drop-down list can now be linked to the **physicalDeliveryOfficeName** attribute.

Linked Combo

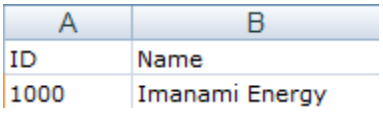
The Linked Combo is a custom display type that can be linked to other display types on a form. When the selected value of the linked combo changes, the values for the display types linked to it change automatically. A common use of this on user interfaces is with the city, state and country fields; for example, when the selected country is changed, the state field changes with it to display states specific to it.

Though the values for the display types linked to a linked combo are updated accordingly, their visual response may or may not be immediate. This depends on the type of display type that is linked. If the linked display type is a combo, the visual response will be immediate. If the linked display type is text, the visual response will not be immediate. You will have to save and reload the form to see the updated value. This behavior of the text display type is due to its limitation to show a single value at a time.

The linked combo requires an XML file which contains the data for the display type itself and the other display types that will be linked to it. For the convenience of users, GroupID also supports the Microsoft Excel file format (.xls) which it automatically converts to XML. The data in the Excel file needs to be in a specific format for GroupID to successfully process it. The following section provides more information on how to prepare this file.

Excel Data File Format

The following table explains the rules for Microsoft Excel workbook.

No.	Rule for	Description
1.	Worksheet names	The worksheet names need to be in the following format: ***Number-Name*** Where: • *Number* is the serial number based on the order of the worksheet and it should start from zero that is the number for the first worksheet should be 0 and then increment by one for each following worksheet. • *Name* is the name of the worksheet that identifies the data it contains. It can be anything you want. **Figure - Shows the worksheet names set for the data file.**
2.	Identity column	Each worksheet needs to have an identity (**ID**) column which will contain a unique value for every record entered in the sheet.  **Figure - Shows the ID column for the 0-Company worksheet.**
3.	Name column	Each worksheet also needs to have a **Name** column. This column contains the actual values that will show in the linked combo. For example, the name column on the 0-Company worksheet will contain the country name for every record on the sheet.
4.	Foreign Key column	Each worksheet that contains data related to that on the previous sheet, needs to have a foreign key identity column (**FK**). This column contains the ID of the record from the previous sheet with which the current record is related.

No.	Rule for	Description
		A / B / C / D FK / ID / Name / State 1000 / 1010 / United States / CA 1000 / 1020 / United States / TX 2000 / 2010 / Canada / ON 3000 / 3010 / Pakistan / PU 3000 / 3020 / Pakistan / ICT 4000 / 4010 / Australia / ACT **Figure - Shows the FK column containing the company ID.**

Creating a Linked Combo

Before creating a linked combo, you should have the data file ready. The data file is used to populate the linked combo itself and the other display types that will be linked to it.

The following instructions list the process for creating a linked combo to define relationship between company, country, state and city fields that appear on the User and Contact forms of the Portal.

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node.
3. Expand the required Portal node and click the **Design** node.
4. Click the **Custom Display Types** tab.
5. In the **Linked Combo Types** area, click **Add**.

Figure - Linked Combo Types area.

6. On the **New Linked Combo Display Type** wizard:
   i. On the welcome page of the wizard, click **Next** to continue.
   ii. On the **Type Name** page, type the name you want to give to this new linked combo, and then click **Next**.

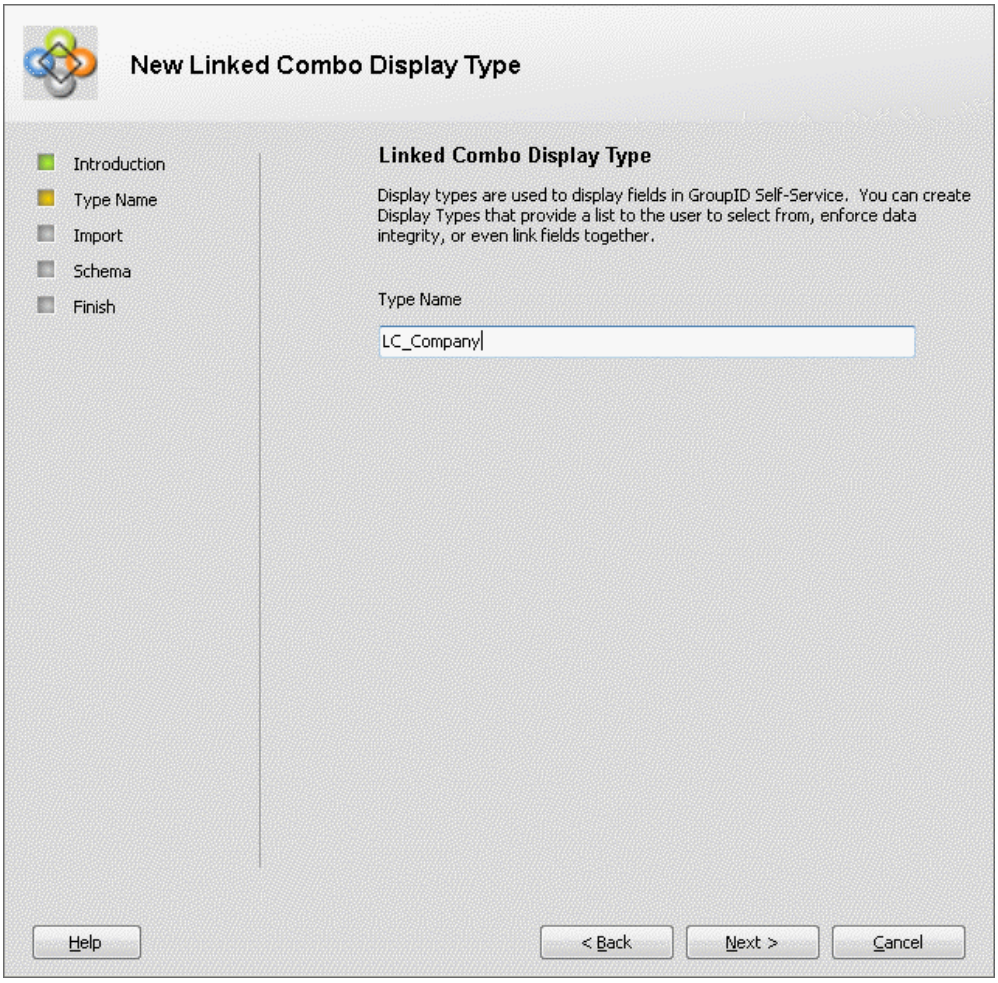

New Linked Combo Display Type
Introduction
Type Name
Import
Schema
Finish
Linked Combo Display Type
Display types are used to display fields in GroupID Self-Service. You can create Display Types that provide a list to the user to select from, enforce data integrity, or even link fields together.
Type Name
LC_Company
Help
< Back
Next >
Cancel

Figure - The Type Name page.

iii. On the **Import** page, click **Browse** and select the XML or Microsoft Excel file containing the data to populate the linked combo and the other display types linked to it.
If your input file is a Microsoft Excel (.xls) file, the wizard will automatically create its XML version.

If data in the source file is updated, the updates will not show in the linked combo or its linked display types until the linked combo is edited and the source file is again selected using the **Import** page. This needs to be done every time you make changes to the data.

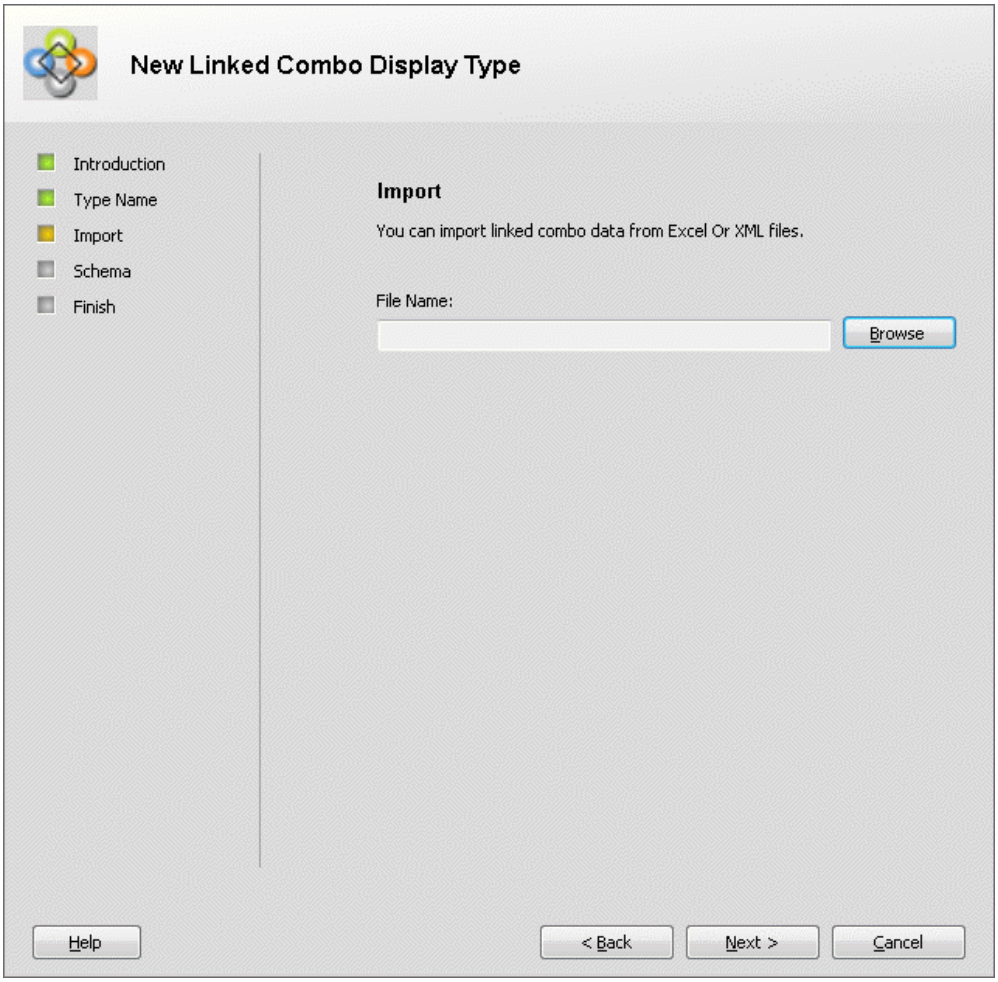


Figure - The Import page.

iv. Click **Next** to continue.

v. On the **Schema** page, specify the relationship between the linked fields from the data file. To learn more, see the section Defining the Linked Combo Schema.

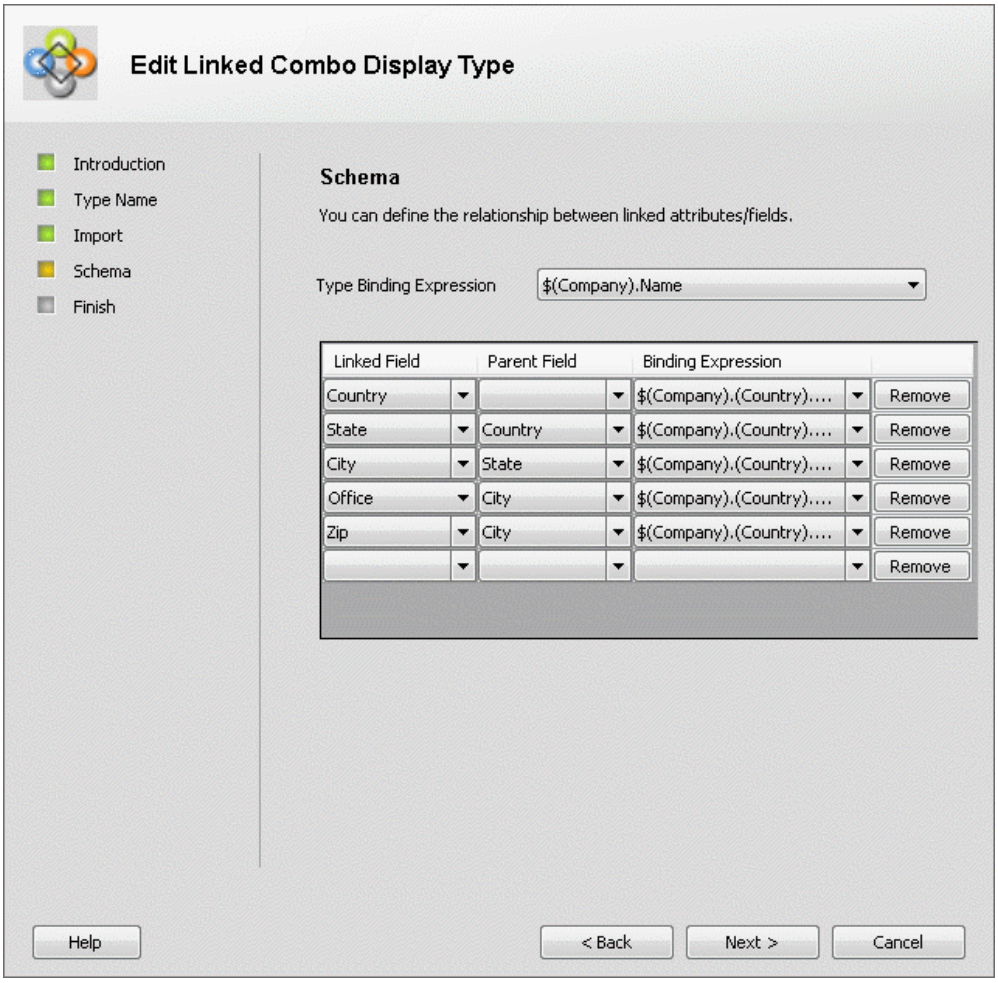


Figure - The Schema page.

vi. Click **Next**.

vii. On the **Confirmation** page, view the detail of your selections on the previous pages and click **Finish**.

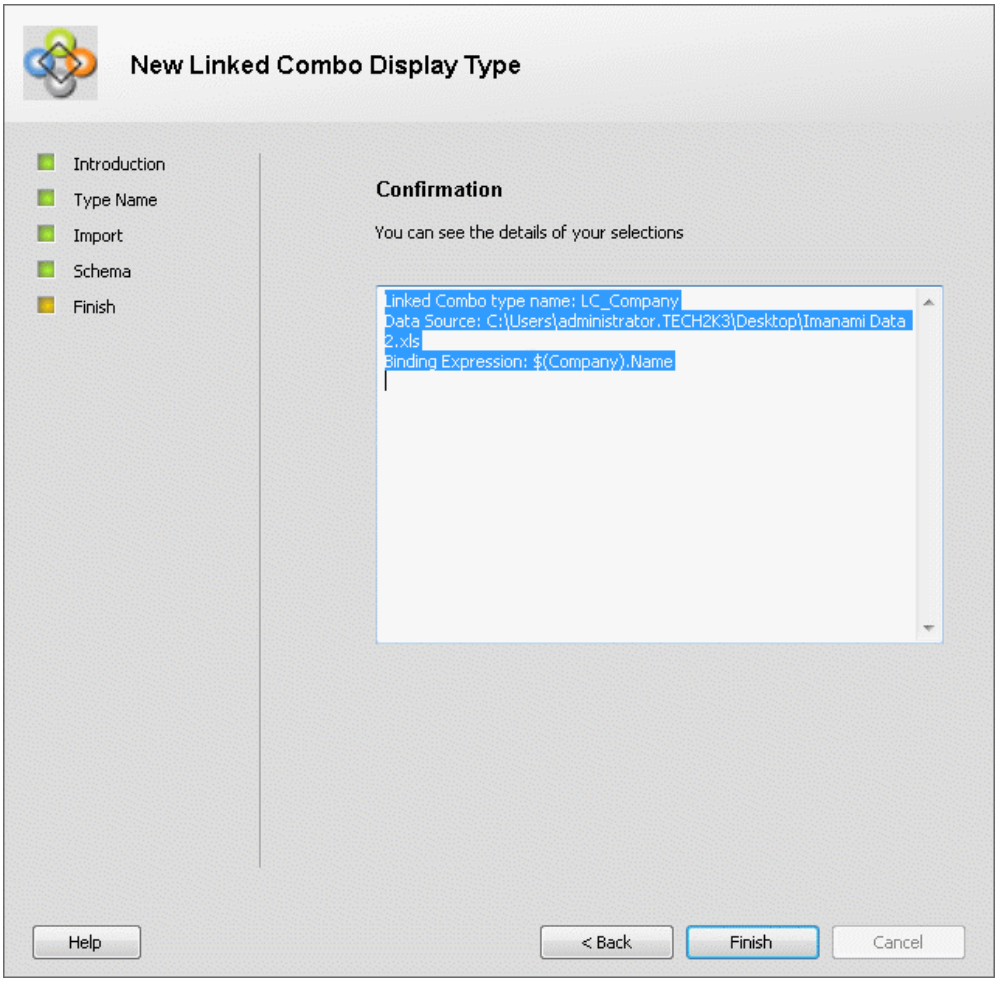


Figure - The Confirmation page.

Defining the Linked Combo Schema

Developing an understanding of how to link fields when defining the schema for a Linked Combo is extremely important to obtain the required behavior of the other display types connected to it. Mapping of fields on the **Schema** page of the **New** or **Edit Linked Combo Display Type** wizard has to be in accordance with how the data has been defined in the source file.

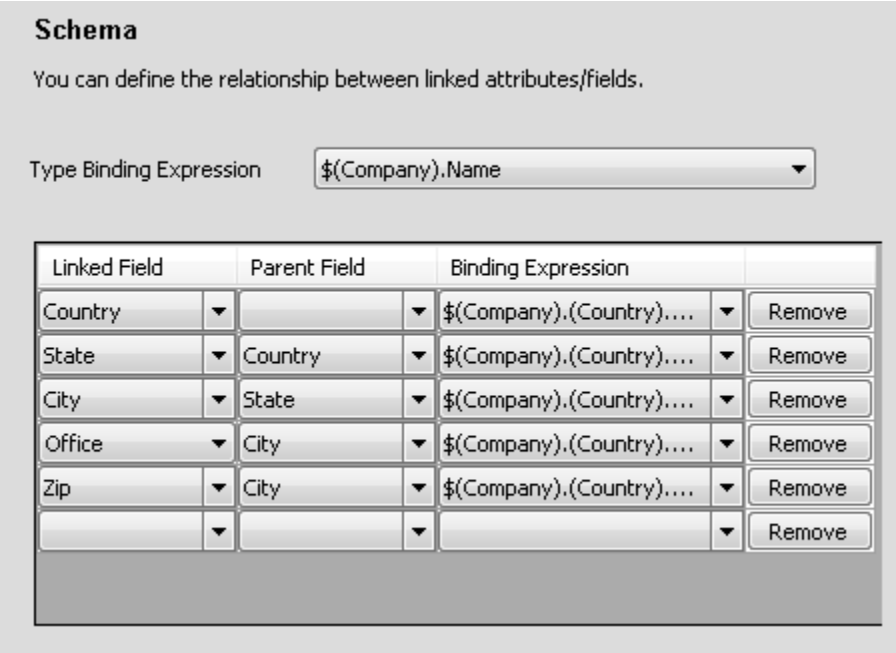


Figure - The Schema Page

The **Type Binding Expression** list on the **Schema** page will be mapped to the very first worksheet (0-worksheet name) of the source Excel workbook. The Type Binding Expression or simply the Binding Expression is used by the display types to obtain reference to the location in the source file from where they are to retrieve and display data.

The grid on the **Schema** page is to link and relate the data from the other sheets of the Excel file to the main content. Use the **Linked Field** column to select the name of the sheet or column to link to the main entity. Similarly, use the **Parent Field** column to select the name of the parent sheet for the linked field.

For example, the schema given in the screen shot above is for an Excel workbook that contains three worksheets; 0-Company, 1-Country, 2-City. The complete structure for the data in the Excel file is explained in the following table.

Worksheet	Columns	Description	Example
0-Company	ID	Company identifier.	1000 2000
	Name	Company name.	Imanami Consulting Imanami Software
1-Country	FK	Company identifier with which to link this record.	1000 2000
	ID	Country identifier.	1010 2010
	Name	Country name.	United States Pakistan

Worksheet	Columns	Description	Example
	State	State abbreviation.	CA PU
2-City	FK	Country identifier with which to link this record.	1010 2010
	ID	City identifier.	1011 2011
	Name	City name.	Livermore Lahore
	Address	Office address 1	5099 Preston Ave. Saddiq Trade Center
	Address 2	Office address 2	
	Zip Code	Postal zip code or area code.	94551 54600

Using the Linked Combo

To use a linked combo, you need to set the display type property of the field to use it with to the name of your linked combo. You also need to set the display types of the other fields associated with this linked combo to a Textbox or Dropdown list depending on whether they will be having single or multiple values.

Moving forward with our example of office, country, state and city which we have been using in the screen shots and explanation in the sections covering this topic; let us now apply the linked combo to the Properties page for the user object. The following instructions list the procedure for setting the linked combo display type for the Company field:

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node.
3. Expand the required Portal node and click the **Design** node.
4. Click the **Properties** tab.
5. Make sure that the selected item in the **Select Directory Object** list is **User**.
6. Double-click **General** to open the fields in this category for editing.
7. On the **Edit Design Category** dialog box, from the **Fields** list, double-click **Company** to open it for editing.
8. On the **Edit Field** dialog box, from the **Display Type** list, select the name of your linked combo display type.
9. Click **OK** on the opened dialog boxes to close them..
10. On the toolbar, click **Save** .

Similarly, you need to set the display types for the rest of the fields. See the following table that mentions the field names and the display types to set for them.

Field	Display Type to set	Notes
Country	Dropdown List	It is recommended that you create a new Dropdown List display type and set that for this field. The default dropdown list, lstCountry, set for this field has default values set for it which may produce undesirable results.
State	Textbox	You can also use a dropdown list instead. For a dropdown list, it is recommended to create a new Dropdown List display type and use that instead of the default, lstState, since its default values may result in undesirable behavior of the display type in browser.
City	Dropdown List	
Address	Textbox	
Zip	Textbox	

The rule of thumb is that for every worksheet in the Excel file, except for the first one, you set their display type to Dropdown List. These lists will be populated with the values in the **Name** column of their related worksheet.

Updating the Source Data File

If data in the source file is changed then the file needs to be reloaded using the wizard. The following instructions list the procedure that needs to be repeated whenever there is a change in the data file that needs to be deployed to the portal.

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node.
3. Expand the required Portal node and click the **Design** node.
4. Click the **Custom Display Types** tab.
5. From the **Linked Combo Types** area, double-click the name of the required linked combo.
6. On the **Edit Linked Combo Display Type** wizard, click **Next** until you reach the **Import** page.
7. On the **Import** page, click **Browse** to locate and specify the file to load and then click **Next** to continue.
8. On the **Schema** page, make changes to the relationships if they are required.
9. Click **Next**.
10. On the **Confirmation** page, click **Finish** to end the wizard.
11. On the toolbar, click **Save** .

12. Launch Windows **Command Prompt**, or the **Run** dialog box.
13. Type and run the following command: `iisreset`
14. Launch the Portal and test your updates.

Customize Search Form

The Web interface of Self-Service enables end users to explore and manipulate Active Directory objects. For this purpose, two search forms are provided on the Portal. The availability of these forms depends on the selected functionality mode. For information about functionality modes, see **Self-Service Functionality Modes** in **Chapter 3: Introduction**. For example; there is a search form available for searching Groups; similarly, there is another search form available for searching users, contacts and folders. Search forms provide users the flexibility to search objects by different attributes.

At the same time, administrators have complete control to customize the fields available on the search forms and the fields displayed in their results.

For search form customization, use the instructions given in the following:

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node.
3. Expand the node of the required Portal.
4. Click the **Design** node and then click the **Search Forms** tab. The tab shows the list of all search forms available on the Portal in the **Name** list.

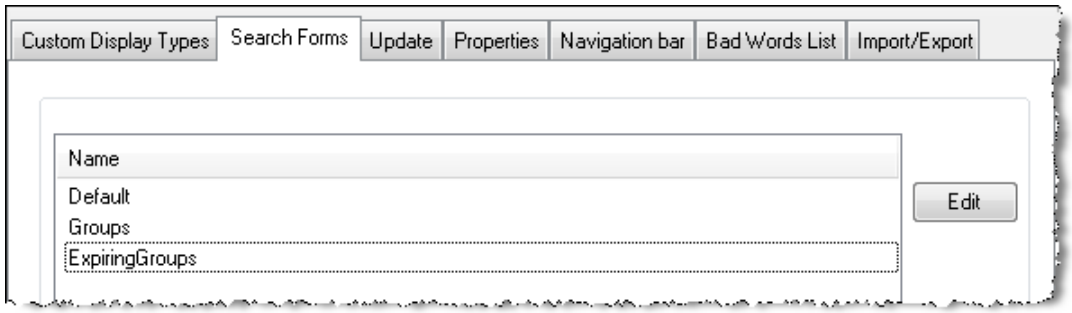


Figure - The Search Forms tab

5. Select the required search form from the **Name** list and click **Edit**. This displays a dialog box showing the current fields list available on the search form and the search results of the Portal. You can add new fields, edit or remove the existing ones. You can also change the order of fields by clicking or buttons.

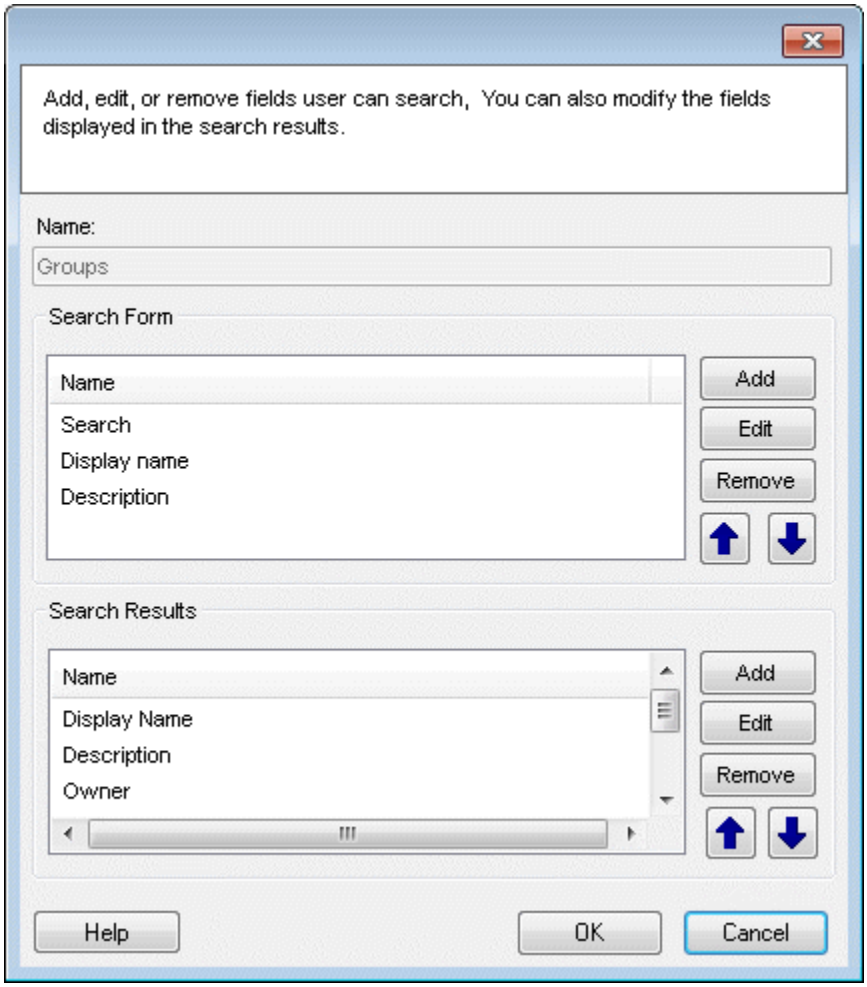


Figure - Dialog box showing the list of current fields for search form and search results

6. To add a new field, click **Add** in the required area. For example; to add a new field for the search form, click Add in the **Search Form** area; similarly, to add a new field for the search results, click Add in the **Search Results** area. This displays another dialog box, on which:

    i. From the **Field** list, select the Active Directory attribute that the new field will represent on the search form or search results.

    ii. In the **Display Name** box, type a display name for the field. This is the name that will show as the label for the field in the search form or search results.

    iii. In the **Tooltip** box, type the ToolTip to show for the field. The ToolTip is the help text that appears when the mouse pointer hovers the field on its Web page. This box is not available when you add or edit the **Search Results** fields.

    iv. In the **Display type** box, select the display type for the field. Display types determine the format of data users can enter for the field. For more information about display type, see **Customize Display Types** earlier in this section. This box is not available when you add or edit the **Search Results** fields.

    v. Click **OK** to close the dialog box.

You can also update and remove fields for search form or search results using **Edit** and **Remove** buttons simultaneously.

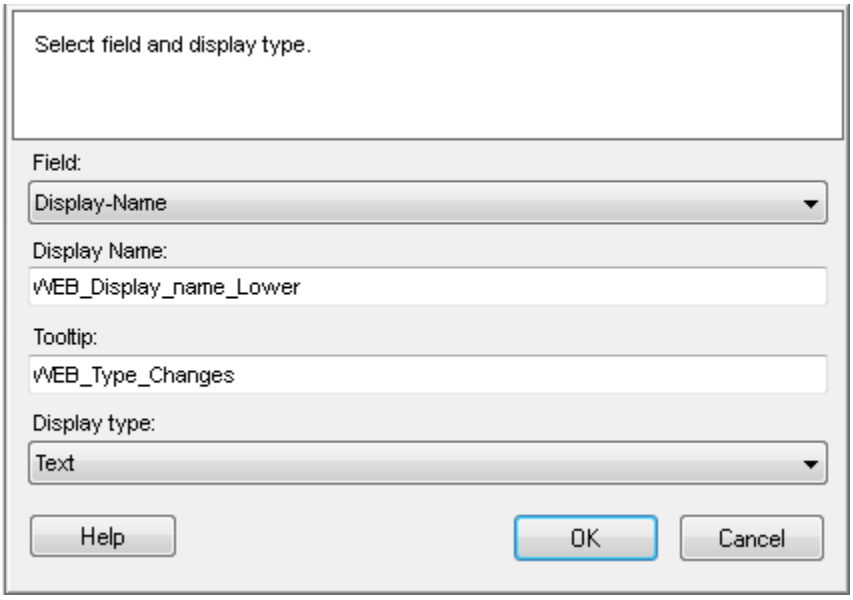


Figure - The dialog box showing details of the field

Customize Update Wizard

The **Update Wizard** allows Portal users to update their profile information using a wizard.

Use the Self-Service administrator from GroupID Management Console to customize the update wizard. The administrator will allow you to change or remove the default pages and fields for the wizard; and even add new pages or fields, if required.

Use the instructions below to customize the wizard:

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node.
3. Expand the node of the required Portal.
4. Click the **Design** node and then click the **Update** tab. The tab shows the list of current pages available on the update wizard in the **Name** list. The pages are referred to as **Categories**.

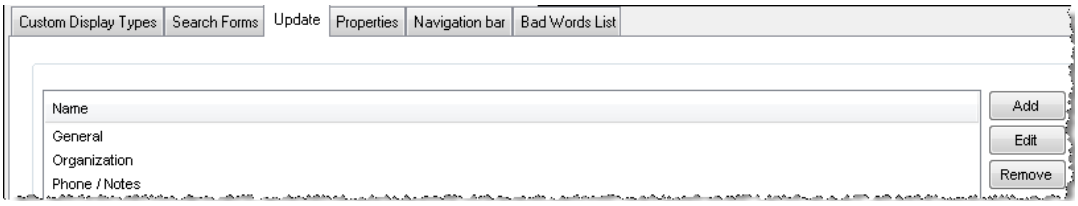


Figure - The Update tab.

To add a new category

1. Click **Add** on the **Update** tab. This displays the **Add Category** dialog box. On the dialog box, provide the following information:

i. In the **Name** box, type the name of the category. The page will appear in the wizard with this name.

ii. In the **Access Level** box, type or select the value in the range 1 to 9999 to set for access level. The access level determines whether a user will be able to modify the fields in a category. The lower the access level, the more restricted is the user and with that they may not be able to modify the fields in the category themselves. Access level examples are:

- **9999** - Anonymous
- **999** - Any user
- **399** - Manager
- **299** - Self
- **199** - Owner
- **99** - Help Desk
- **1** - Administrators
- **0** - Read Only

iii. In the **Visibility Level** box, type or select the value in the range of 0 to 9999 as the visibility level. The Visibility level determines whether a user will be able to view a category or a field in that category. This rule also applies to Access level i.e. the lower the access level will restrict the number of people that can view or access the category or field.

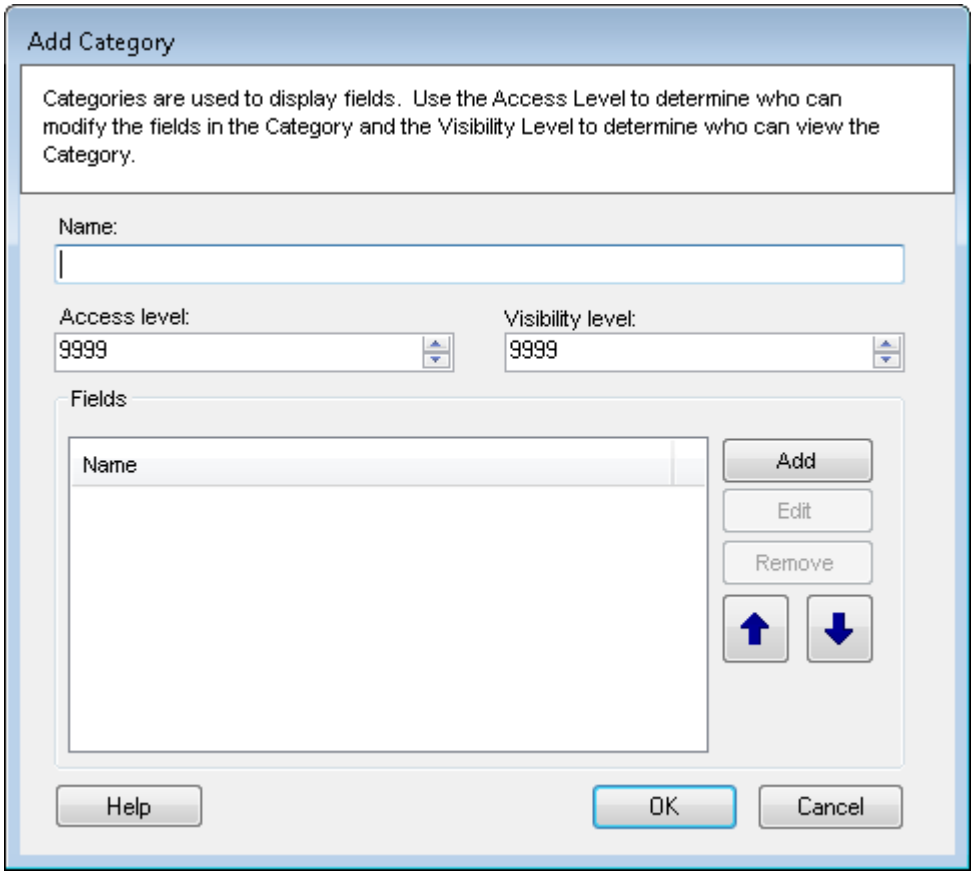


Figure - The Add Category dialog box.

To add a field in the category

1. In the **Fields** area, click **Add**. This displays the **Edit Field** dialog box. On the dialog box:

    i. From the **Field** list, select the Active Directory attribute that the new field will represent on the category.

    ii. In the **Display name** box, type a display name for the field. This is the name that will show as the label for the field.

    iii. In the **ToolTip** box, type the help message to show for the field. The ToolTip is the help message that appears when the mouse pointer hovers over the field.

    iv. In the **Display type** box, select the display type for the field. Display types determine the format of data users can enter for the field. For more information about display type, see **Display Types** earlier in this section.

    v. In the **Access Level** box, type or select the required access level. Access levels are explained earlier in this topic.

    vi. In the **Visibility Level** box, type or select the required visibility level. Visibility levels are explained earlier in this topic.

    vii. Select the **Value Required** check box if you want to make the field mandatory.

    viii. Click **OK** to close the **Edit Field** dialog box.

Following the above procedure, you can add as many fields as required for the category. You can also change the order of fields by clicking or buttons.

You can edit a field by selecting it and clicking **Edit**. This displays the **Edit Field** dialog box where you can edit the required information. A field can be deleted by selecting it and clicking **Delete**.

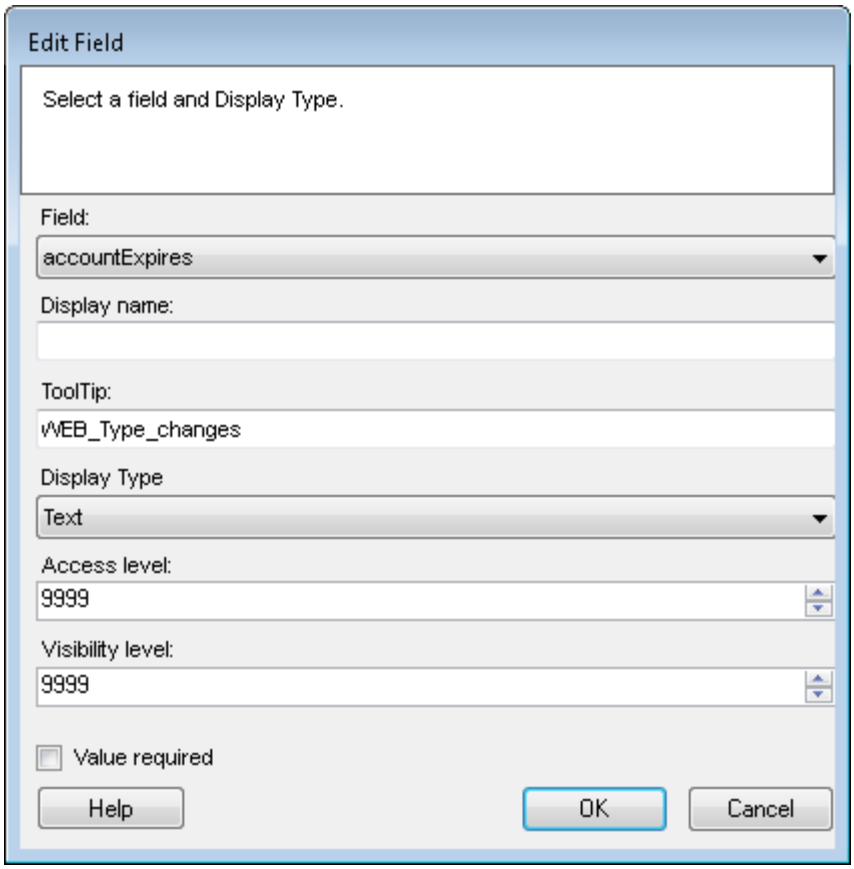


Figure - The Edit Field dialog box.

Customize My Properties

In Active Directory concepts, the term **Properties** represents the attributes of an object. In the Active Directory Management Console, the object properties are displayed on a tabbed dialog box with each tab grouping the related attributes of the object. Self-Service Portal follows the same design for displaying the property pages of objects like Users, Groups, Contacts and Folders.

You can control the property pages and the attributes to display on them using the GroupID Management Console. The following instructions list the procedure for customizing these properties:

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the required portal.
3. Click the **Design** node and then click the **Properties** tab.

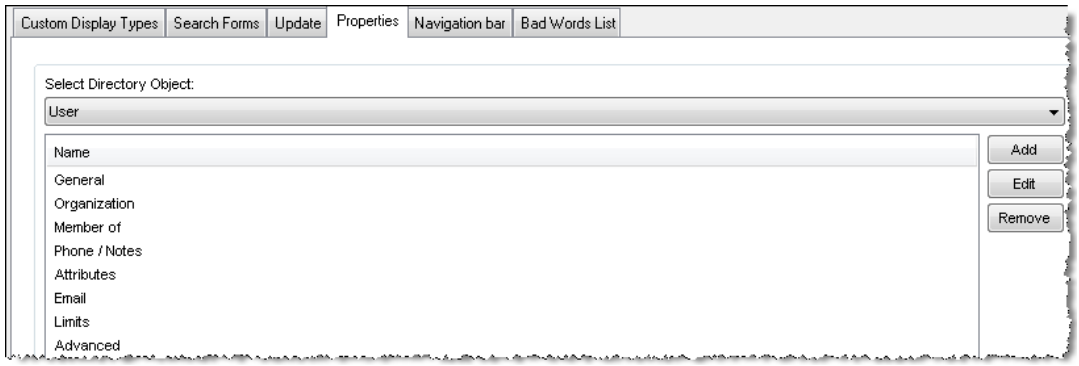


Figure - The Properties tab

4. Select an object from the **Select Directory Object** box and the **Tab Name** list will show the tabs for the object.

5. Use the same procedure as mentioned earlier in **Customize Update Wizard** section to manipulate categories and fields.

Navigation Bar

Navigation bar refers to the left navigation bar on a Portal that, by default, contains links to other pages of the Portal for interacting with the Active Directory objects. The navigation bar is available on every page and forms the main navigational component of the user interface.

Home
Log Off
GroupID
Self-Service
The Navigation bar
Search
Go
Advanced Search
User: Administrator
Options | Help | Contact
Welcome
Groups
My Groups
My Memberships
My Expired Groups
My Expiring Groups
My Deleted Groups
Users
My Profile
My Direct Reports
Change My Password
Reset Password
Requests
Request Inbox
My Requests
History
My History
My Direct Report's History
My Group's History
Recently Viewed
Groups
Groups are primarily used for sending email to distribution lists and to secure network resources. Any group that you create can be found in the Global Address List. As the owner of a group, you will want to manage the membership of that group. As a user, you may want to request membership into a group. All of these functions and more can be managed through the Groups interface.
Create a new group
Manage my groups
See my group memberships
Join a group
Users
Your profile information is a key aspect to communication. GroupID allows you to manage all of your contact information, ensuring that your address, phone numbers, and email address are always correct for your colleagues. Look up other employees and make sure they can find you by keeping your information up to date.
Edit my profile
Manage my direct reports
Find People
Create a new user
Create a new mailbox
Create a new contact
Requests
Requests are approvals to changes that need to happen. You will find the requests that you need to approve and can keep track of requests that you've made.
Approve requests
My Requests
History
Out of bound reached for group OOB 5 hour(s) ago.
Out of bound reached for group SchedulingTest 5 hour(s) ago.
My History
My Groups History
My Direct Reports History
Help
Change my start page or other options
GroupID Help
Powered by Imanami GroupID Self-Service 6.0.3992.2
Copyright © 2001-2010 Imanami Corporation. All rights reserved.

Figure - The navigation bar in focus.

The contents of the navigation bar are fully customizable for all functionality modes. Links can be removed, added, or hidden as required. Administrators can customize the text for links, control their access levels and set them to open in a new browser window.

The settings for navigation bar are available from **Design** node of a Portal. The following sections provide instructions for viewing the settings and customizing the navigation by adding or removing links.

To view the navigation bar settings

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node.
3. Expand the node of the required Portal.
4. Click the **Design** node and then click the **Navigation bar** tab.
   A list of Tabs for the selected mode will be displayed. The term Tab here refers to the collection of similar links which appear under the same header in the Portal.

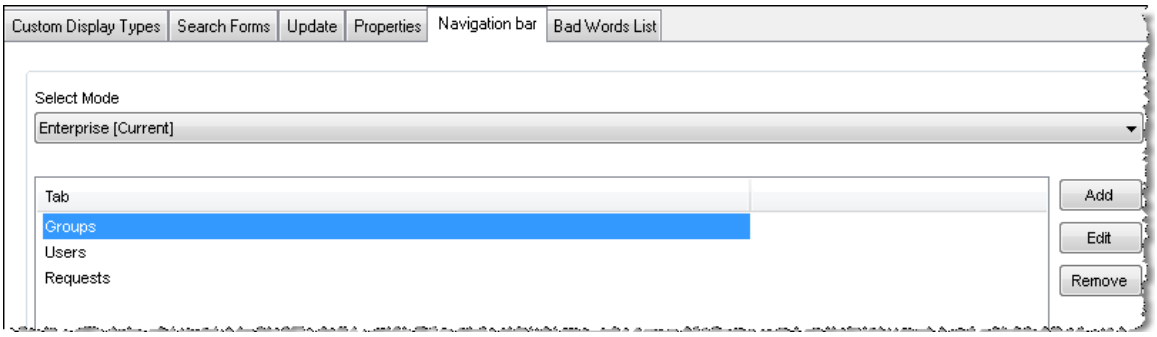


Figure - The Navigation bar tab.

To add a new tab

1. On the **Navigation bar** tab, use the **Select Mode** list to selected the required mode and then click **Add**.
   This opens the **Add Tab** dialog box.

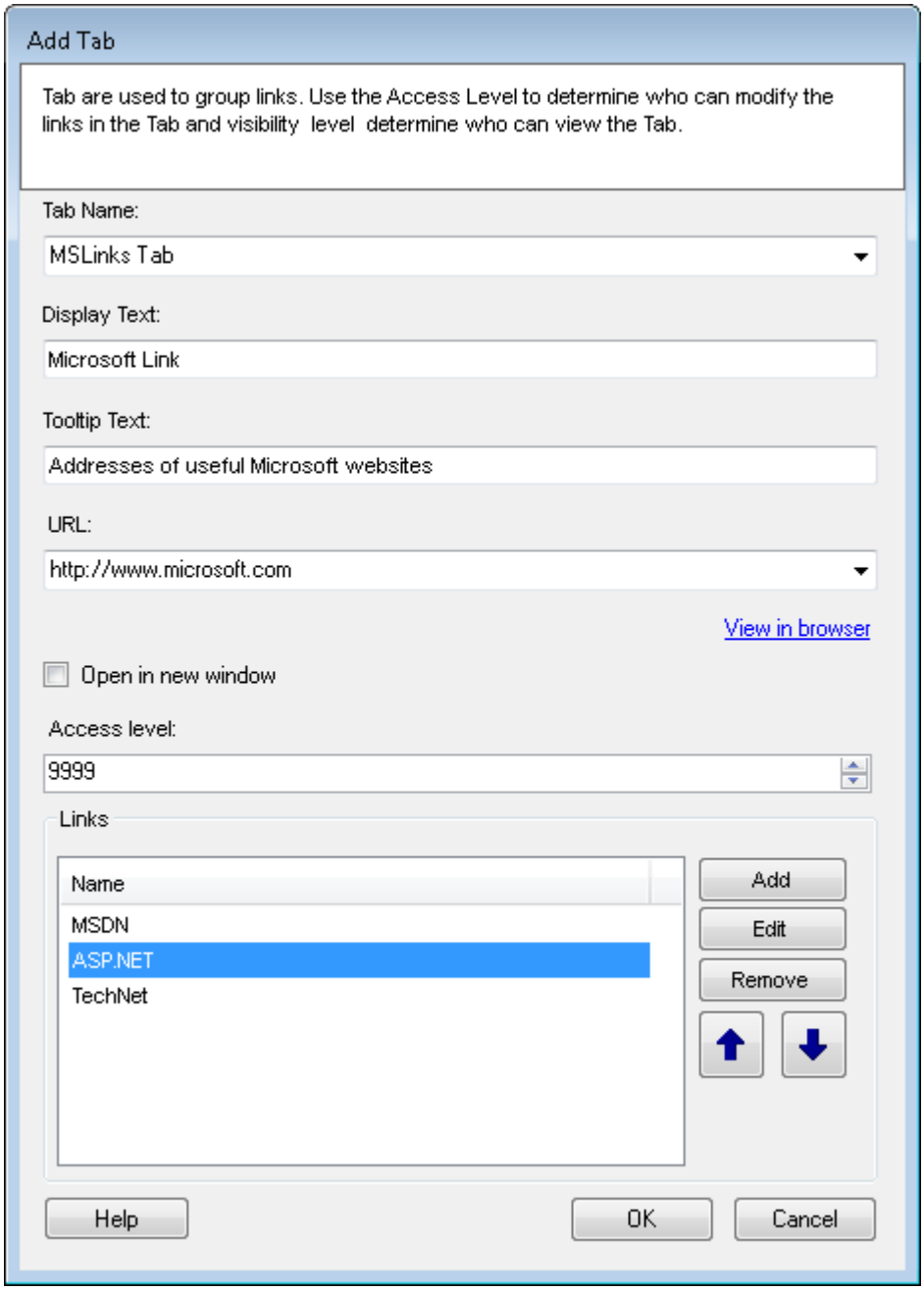


Figure - The Add Tab dialog box.

2. On the **Add Tab** dialog box, enter the following information for the new Tab:

   i. In the **Tab Name** list, type the name for your new Tab. If the Tab to include is a default Tab of the selected mode, you can also use the list to select it.
   The Tab Name is for internal use by GroupID only.

   ii. In the **Display Text** box, type the text to show as the Tab name on the Portal.

   iii. In the **ToolTip** box, type the help message to show for the Tab. The ToolTip is the help message that appears when the mouse pointer hovers over the Tab.

iv. If you want to link the Tab to an internal or external page, enter its address in the **URL** list.

- To link an internal page, select the required page from the list.
- To link to an external page or Web site, type its address.

v. Select the **Open in new window** check box, to open the link (if given) in a new browser window.

vi. In the **Access Level** box, type or select the required access level. Access levels are explained earlier in this chapter.

vii. Use the **Links** section to add, edit or remove links for this Tab.
The steps for adding a link are identical to how a Tab is added. Click **Add** in this section and then follow the steps from (i) to (vi) on the **Add Link** dialog box to add links as required.

viii. Repeat step 2(i) to 2(vii) to add more Tabs and their links. You can also change the order of fields by clicking or buttons.

3. Click **OK** to close the dialog box.
4. On the toolbar, click **Save** .

To modify an existing Tab or its Link

1. On the **Navigation bar** tab, use the **Select Mode** list to select the required mode.
2. In the **Tabs** list, select the required Tab and then click **Edit**.
This opens the **Edit Tab** dialog box. The dialog box is identical to the **Add Tab** dialog box.
3. Use the **Edit Tab** dialog box to make the required changes.
For information about the Tab properties, see instructions for adding a new tab.
4. Use the links section to add, edit or remove links for this Tab.
5. Click **OK** to close the dialog box.
6. On the toolbar, click **Save** .

To remove a Tab

Simply select the Tab for the selected mode and then click **Remove**. Removing a tab will remove all its links with it. You can also delete default Tabs and Links.

To re-add a Tab

A default Tab that has been removed can easily be re-added by selecting the name of the Tab from the **Tab Name** list on the **Add Tab** dialog box. This will also add all the default links for this Tab.

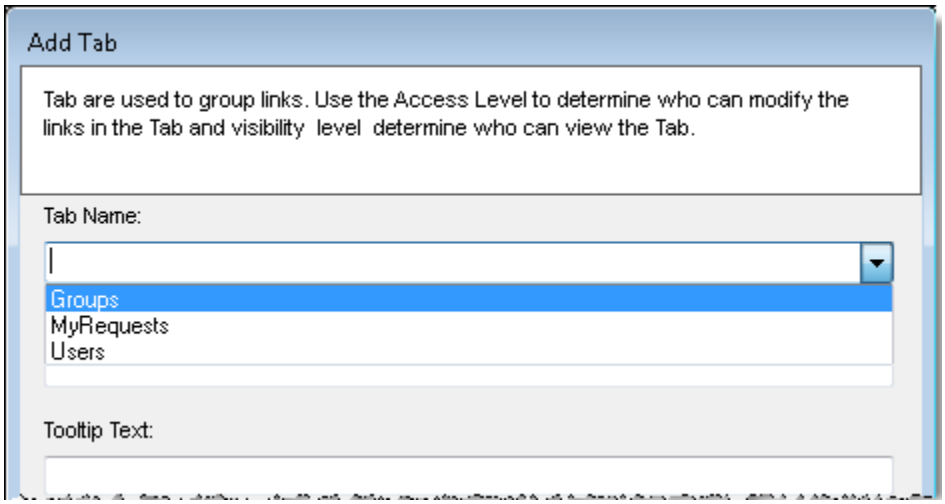

Add Tab
Tab are used to group links. Use the Access Level to determine who can modify the links in the Tab and visibility level determine who can view the Tab.
Tab Name:
Groups
MyRequests
Users
Tooltip Text:

Figure - Tab Name list showing the names of the default Tabs for Enterprise mode.

Bad Words List

Users can be restricted from saving data in fields which may consist of words that may be offending. A dictionary of such words can be maintained using the **Bad Words List** tab in the Design settings of a Portal. The Bad Words List feature only works for Group objects and applies only for their name, display name, description, and notes attributes. Any entry in these attributes that is a part of the list cannot be saved until it is removed or corrected.

The following instructions list the procedure for adding words to the Bad Words List:

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the required Portal.
3. Click the **Design** node and then click the **Bad Words List** tab.

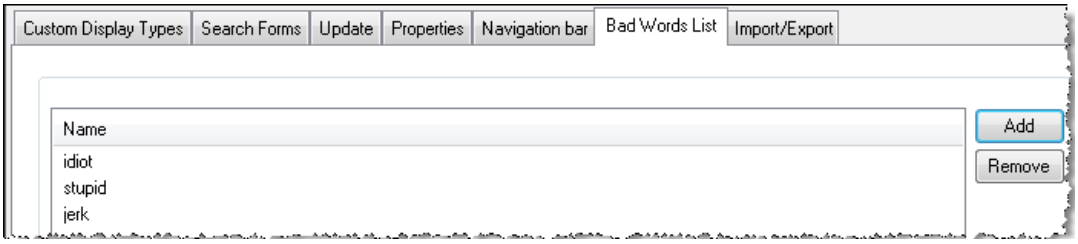


Figure - The Bad Words List tab.

4. Click **Add**.
5. On the **New Bad Word** dialog box, enter your word in the given box, and then click **OK**.
6. Repeat steps 4 to 5 to add more words.
7. On the toolbar, click **Save** .

Make sure that the **Enable Bad Words feature** check box is selected. You can use this check box to enable or disable the enforcement of this list as required.

Figure - The Enable Bad Words feature check box.

This feature does not apply to users with administrative privileges.

Rename Active Directory attributes

This setting is a part of the feature that allows importing and exporting of members and additional owners for a group using the Portal. Both: import and export, involve the selection of attributes for the members or additional owners. When importing, the attributes determine the destination fields with which data from the source fields will be matched. When exporting, data for only the selected attributes is included in the output file.

Since Portals are meant to be used by staff members, who will include non technical users, understanding the use of Active Directory attributes by their original names will be inconvenient for them. Renaming makes it possible to assign easy to understand, or user-friendly names to Active Directory attributes. The assigned names replace the original names in the lists showing Active Directory attributes on the import and export dialog boxes.

To rename an attribute:

1. Launch GroupID Management Console.
2. Under the **Self-Service** node, expand the **Portals** node.
3. Expand the required Portal node and click the **Design** node.
4. Click the **Import/Export** tab.
   The tab, by default, shows you three pre-defined renamed Active Directory attributes.

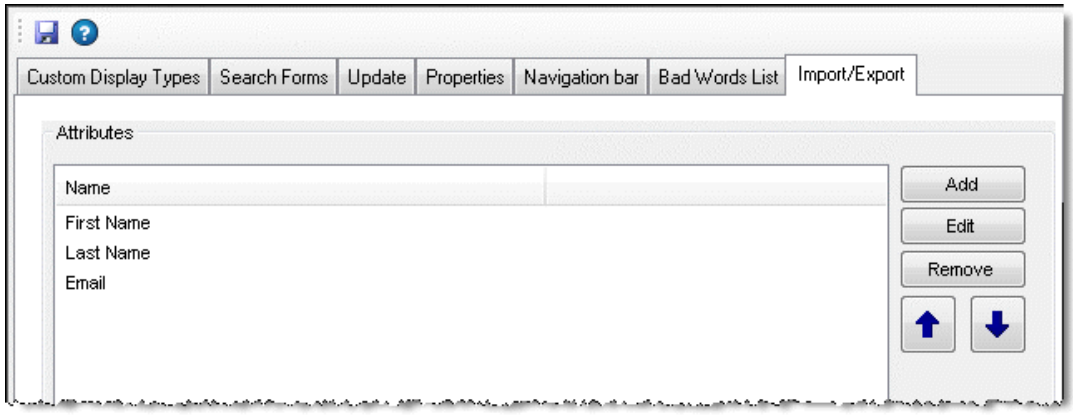


Figure - The Import/Export tab

5. Click **Add**.
   This displays the **Import/Export Attribute** dialog box. On the dialog box:
   i. In the **AD Attribute** list, type or select an Active Directory attribute for which you want to add a user-friendly name.
   ii. in the **User Friendly Name** box, type an easy to understand and meaningful name for the selected Active Directory attribute.

iii. Click **OK**.

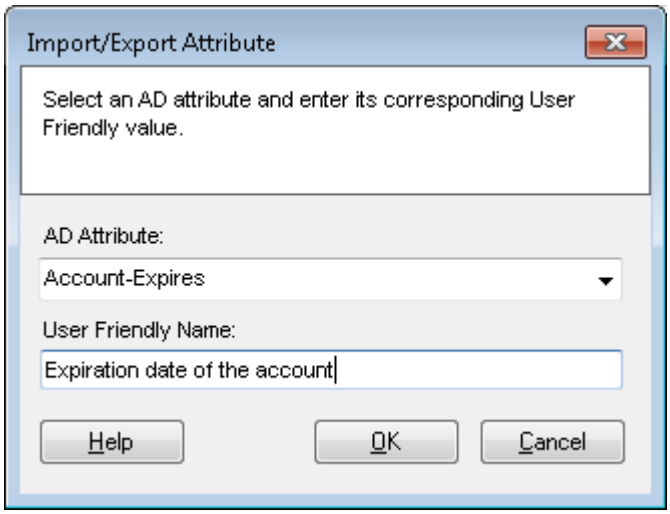


Figure - The Import/Export Attribute dialog box

Part 3 - Automate

This part of the documentation covers the Automate module of GroupID. The detailed information on how Automate helps in intelligent group management is covered.

Chapter 8: Introduction, introduces you to Automate and its user interface elements.

Chapter 9: Managing Groups, provides management information for all group types: unmanaged groups, SmartGroups and query based distribution groups.

Chapter 10: Memberships, explains how the group membership can be managed.

Chapter 11: Exchange, covers Exchange settings available for mail-enabled groups.

Chapter 12: Dynasties, introduces you with Dynasties and covers the options and settings that can be used to enhance its structure.

Chapter 13: The Query Designer, describes the Query Designer, the interface for building custom queries.

Chapter 8: Introduction

This chapter provides a brief overview of Automate. The key concepts that you should be familiar with before using Automate are also covered here. It also helps you to get familiarized with the user interface of Automate. The chapter is divided into the following sections:

Automate, provides a brief overview of Automate.

Getting familiar with the User Interface, introduces you to the Automate interface and will guide you through the process of applying different customizations to it.

Upgrading from Quest ActiveGroups to Automate, provides instructions on how you can upgrade Quest ActiveGroups to Automate.

Automate - Overview

Automate dynamically maintains Active Directory Distribution Lists and Security Groups based on rules that are applied to your directory data. When a user's directory information changes the Automate module will automatically update the appropriate groups thus ensuring that your groups are never out of date.

Automate creates and updates Distribution Lists and/or Security Groups based on a user-defined LDAP query. Automate provides intelligent group management, so administrators can easily maintain large distribution lists and groups without having to manually add and remove members.

Getting familiar with the User Interface

In GroupID Management Console, the **Automate** node is the first module node after **Getting Started** in the tree view. Expand the Automate node to view its sub-nodes. The sub-nodes for Automate are categorized by views which are filtered to show you a list of relevant groups. Right-clicking a node at any level, including the Automate node itself, will display the shortcut menu with commands that you can execute at that level.

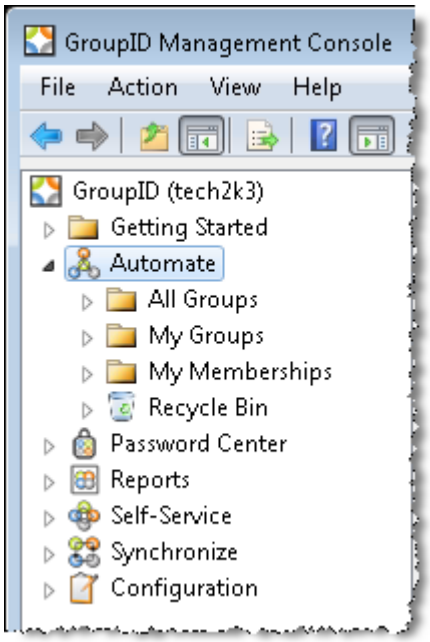


Figure - The Automate node

Following is a summary of the Automate sub-nodes:

Sub-node	Description
All Groups	Shows all groups defined in the specified domain. The list includes all groups whether they are Universal, Global, Local, Private, Public, Expired or still active.
Private Groups	Shows only the private groups. A private group is owner managed. Members can only be added and removed from the group by the owner. Additional owners can also manage membership of the group.
Semi Private Groups	Shows only the semi private groups. The semi private group is similar to a private group, except that an e-mail request is sent to the group owner for approval whenever someone opts to join or leave the group.
Public Groups	Shows only the public groups. A public group is open for all users. Users can join and leave the group at will, since permission is not required.
Semi Public Groups	Shows only the semi public groups. A semi public group is similar to a public group in terms that no restrictions apply when joining or leaving it. However, an e-mail notification is sent to all group owners informing them about the

Sub-node	Description
	membership changes.
Expired Groups	Shows only the expired groups. An expired group is created for a fixed term, which is determined by the expiration policy that is set by the group owner. An expiration policy is a period of time which defines the lifecycle of a group. Once the period ends the group is locked down to prevent any further activity from occurring until the group is renewed. If an expired group is not renewed after a period of time it is automatically deleted from Active Directory.
Smart Groups	Shows only the managed groups created by the Automate module. SmartGroups are ones that dynamically maintain their distribution list and security group memberships based on rules applied with a user-defined LDAP query. When a managed group is scheduled to run, it will apply the rule defined to execute the membership update.
Dynasties	Shows only the Dynasties created by the Automate module. A dynasty is a distribution list that creates and manages other distribution lists using the information in Active Directory.
My Groups	Shows all groups owned by the current logged on user.
My Memberships	Shows all groups that the current logged on user is a member of.
Recycle bin	Shows physically deleted groups.

Sorting the Groups List

By default, groups list is sorted by the group name in ascending order. You can sort the list by any other field according to your requirement. The instructions below guide you on how you can apply sorting to groups list:

1. Expand the **Automate** node and select the required group node on which you want to apply sorting.
2. On the groups list, click on a column header to sort the groups. For example, click the **Owner** column header to sort the groups by owner. Clicking once on an unsorted column header arranges the list in ascending order and clicking again sorts it in descending order.

Apply Filters to the Groups List

Each groups list, by default, shows all relevant groups based on the maximum limit set for displaying groups. For information about setting the display limit, see **Setting Maximum Items to Display in Groups List** later in this section. Assume that your groups list has 500 groups and you would like to see all of the groups that will expire in the next 30 days. This scenario can be handled in Automate by using a **Filter**. Filters help you narrow-down groups list based on any given criteria. Criteria are composed of three items: Field, Condition and Value. **Field** describes the attribute (Active Directory or Exchange) on which you want to apply the filter. **Condition** describes the operator or rule that you want to apply to the selected field. **Value** describes the parameter that the condition uses to short-list groups.

Use the instructions below to apply filters:

1. Expand the **Automate** node and select the required group node.
2. Click **Create Filter**. This shows a row of fields for specifying the filter expression.
3. From the first list, select the field name on which to apply the filter.
4. From the second list, select the operator to apply on the selected field.
5. In the third field, type or select the value (not case-sensitive) that determines whether the condition satisfies the requirement for this filter. For some operators this field will become unavailable, such as in the case of **is present** or **is not present**. Both conditions use a wildcard to return all items that fit the criteria.
6. Click **Apply Filter**.

This will return the results based on the applied filters. You can apply more filters to the list by clicking **Add Expression** and repeating steps 3 to 6. Each additional filter applied will be combined with the others to return results that match all the given filters. You can remove a filter by clicking next to the required filter. All filters can be removed by clicking **Remove Filter**.

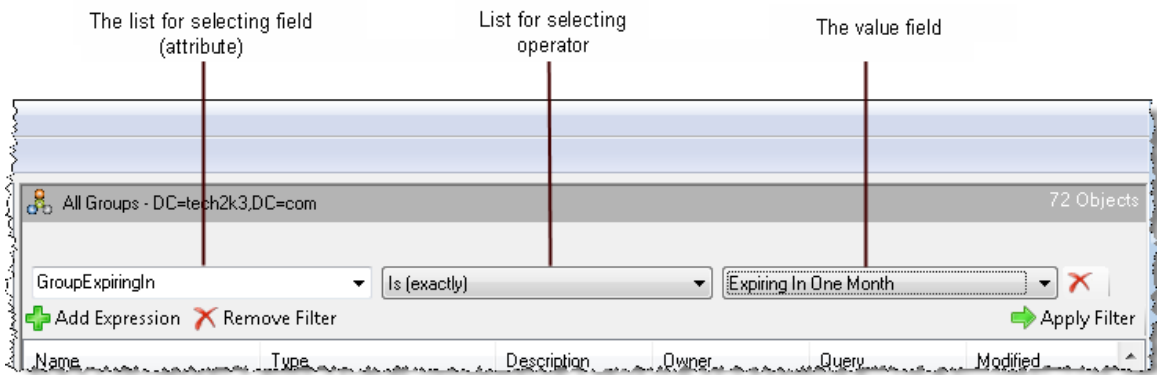


Figure - The area for providing filter criteria

Setting Maximum Items to Display in Groups List

The maximum number of groups to display within the groups list is set to 1000, by default. This number can be changed as required. There is an Active Directory setting that stores the maximum objects limit in the server registry. You can directly modify the registry to define or update the objects limit.

To change the default number of items for groups list, use the instructions given in the following:

1. In the tree-view of GroupID Management Console, expand the **Automate** node.
2. Right-click **All Groups**, and then click **Modify Maximum Items to display**.
3. On the **Maximum Number of Items to be Displayed** dialog box:
    i. In the **Maximum items to display** box, type the number of items you want to display on the groups list.
    ii. Click **OK**.

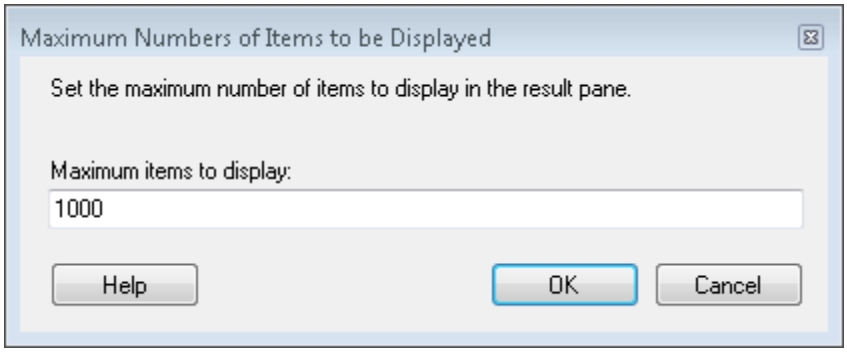


Figure - The Maximum Number of Items to be Displayed dialog box

Modify maximum objects limit at Active Directory

1. Open **Active Directory Users and Computers** from **Administrative Tools**.
2. Right-click the domain node and click **Properties**.
3. On the domain properties dialog box, click the **Group Policy** tab.
4. Select the Group Policy Object, and click **Edit**. This displays the **Group Policy Object Editor**. On the Editor:

i. Expand **User Configuration**, **Administrative Templates**, **Desktop**, **Active Directory**.

ii. Double-click **Maximum size of Active Directory searches**.

iii. Click **Enabled**.

iv. In the **Number of objects returned** box, type or select the required number of objects that you want to set as the maximum limit for the Active Directory.

v. Click **Apply** and then click **OK**.

vi. Close the Editor.

This change will take effect when you log on to the domain next time.

Edit registry to specify objects limit

1. Open the **Registry Editor** by typing **regedit** in the Windows **Run** dialog box.
2. Expand **HKEY_CURRENT_USER**, **Software**, **Policies**, **Microsoft**.
3. Under **Microsoft**, locate the **Windows** key. If not found, add a new registry key with this name using the instructions below:
   - Right-click **Microsoft**, point to **New** and then click **Key**.
   - Type **Windows**.
4. Under **Windows**, locate the **Directory UI** key. If not found, add a new registry key with this name using the instructions below:
   - Right-click **Windows**, point to **New** and then click **Key**.
   - Type **Directory UI**.
5. Click the **Directory UI** key and locate the **QueryLimit** DWORD Value. If not found, add a new DWORD Value with this name using the instructions below:
   - Right-click **Directory UI**, point to **New** and then click **DWORD Value**.
   - Type **QueryLimit** and press **Enter**.
6. Double-click **QueryLimit**. On the **Edit DWORD Value** dialog box:
   i. In the **Base** area, click **Decimal**.
   ii. In the **Value data** box, type the required number that you want to set as the object limit.
   iii. Click **OK**.
7. Close the **Registry Editor**.

This change will take effect when you log on to the domain next time.

Change Group Scope

The default setting of Automate shows recipients from the entire Global Catalog. You can limit this display scope to a single domain or even an organizational unit to save network bandwidth and resources.

Use the instructions given in the following to change the group scope:

- Expand the **Automate** node, right-click **All Groups** and then click **Modify Group Scope**. This displays the **Recipient Scope** dialog box. On the dialog box:

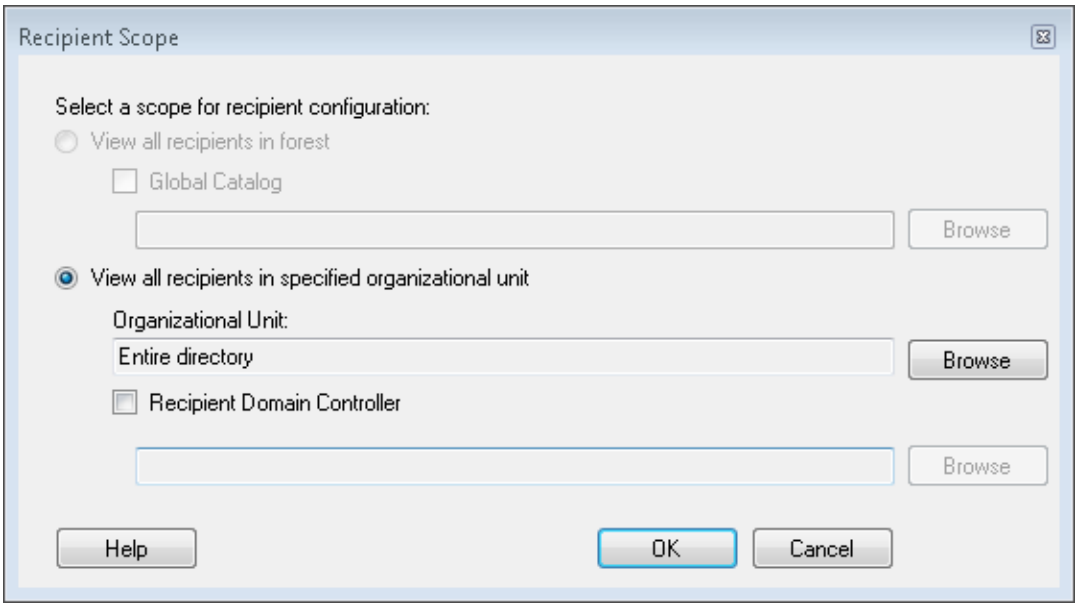


Figure - The Recipient Scope dialog box

To change the scope to an organizational unit

- Click **Browse** beside the **Organizational Unit** box. This displays the **Select container** dialog box where you can select the required container.
- Click **OK** to close the dialog box.

To change the source domain

- Select the Recipient Domain Controller check box. This enables the Browse button.
- Click **Browse** to display the **Select Domain Controller** dialog box where you can select the required domain.

  Only the domains present in the Active Directory forest, which the domain controller for GroupID is connected to will be shown on the dialog box.

- Click **OK** to close the dialog box.

Active Directory and Exchange Permissions for Automate

The recommended permissions for an Automate user is Domain Admin in Active Directory. However, non-administrative users can also use Automate for creating and managing group information, if they have following permissions:

Active Directory Permissions

Permission	Type	Applied to
Create Group Objects	Allow	This object only
List Contents	Allow	This object and all child objects
Read All Properties	Allow	This object and all child objects
Write All Properties	Allow	This object and all child objects
Read Permissions	Allow	This object and all child objects
All Validated Writes	Allow	This object and all child objects

Exchange Permissions

If Exchange Server is deployed on the server, the user account should have the **Exchange View-Only Administrator** role at the Exchange Organization level.

General Permissions

On a member server or workstation, the user account should be the member of the local machine's **Administrators** group where GroupID is installed.

Upgrading from Quest ActiveGroups to Automate

GroupID Automate not only recognizes Quest ActiveGroups and shows them, but it can also upgrade them for you to its native format so you are able to manage them through it. If you choose not to upgrade your ActiveGroups, Automate will display them as unmanaged groups and will message you to upgrade them when you try to modify them.

> Upgrading of ActiveGroups to GroupID is an irreversible process. Imanami suggests taking the necessary precautions before proceeding to avoid any inconvenience.

The following steps list the procedure for upgrading Quest ActiveGroups:

1. From GroupID Management Console, expand the **Automate** node.
2. Right-click **All Groups**, and then click **Import Active Groups Wizard**.

3. On the **Welcome** page, read the message and click **Next**.

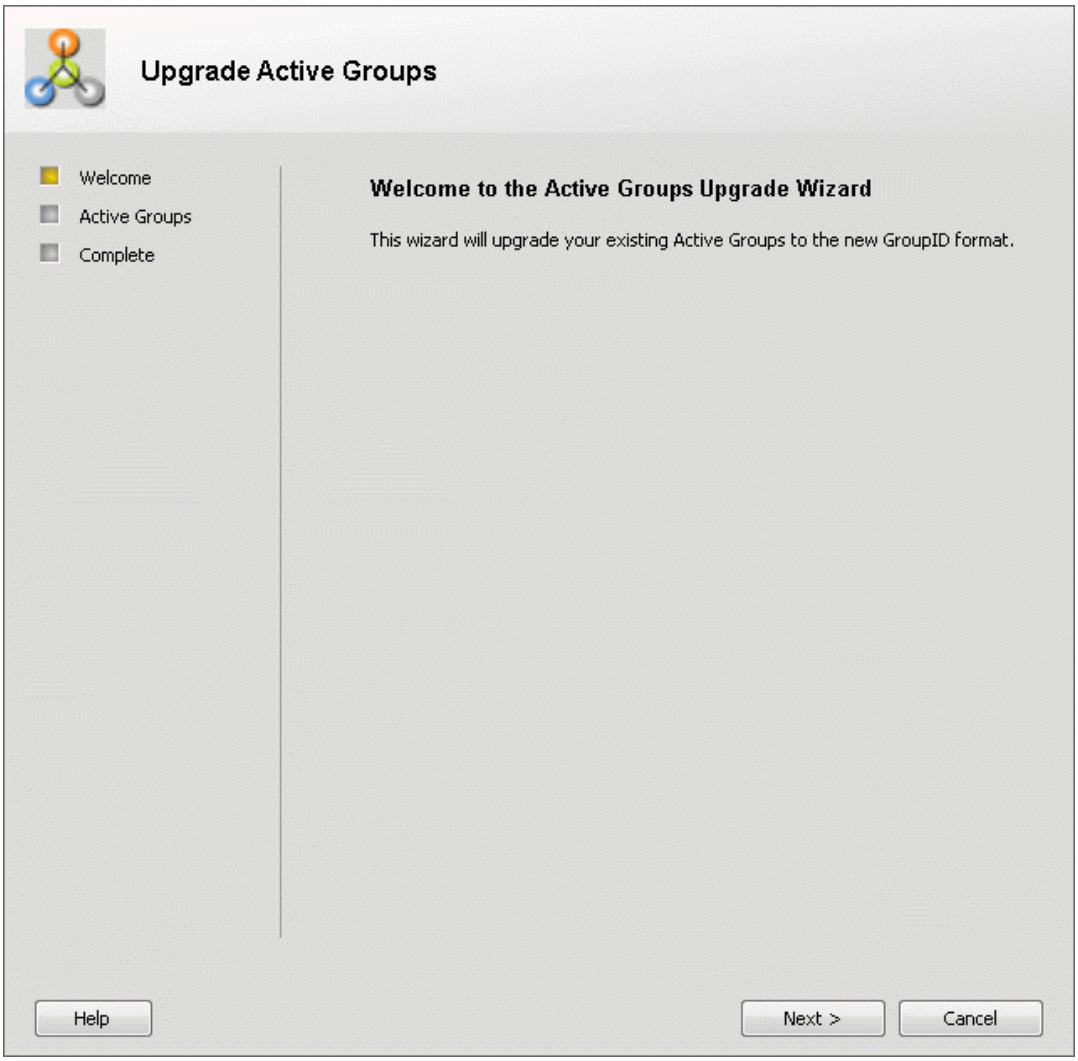


Figure - The Welcome page

4. On the **Active Groups** page, select the groups to upgrade and then click **Next**.

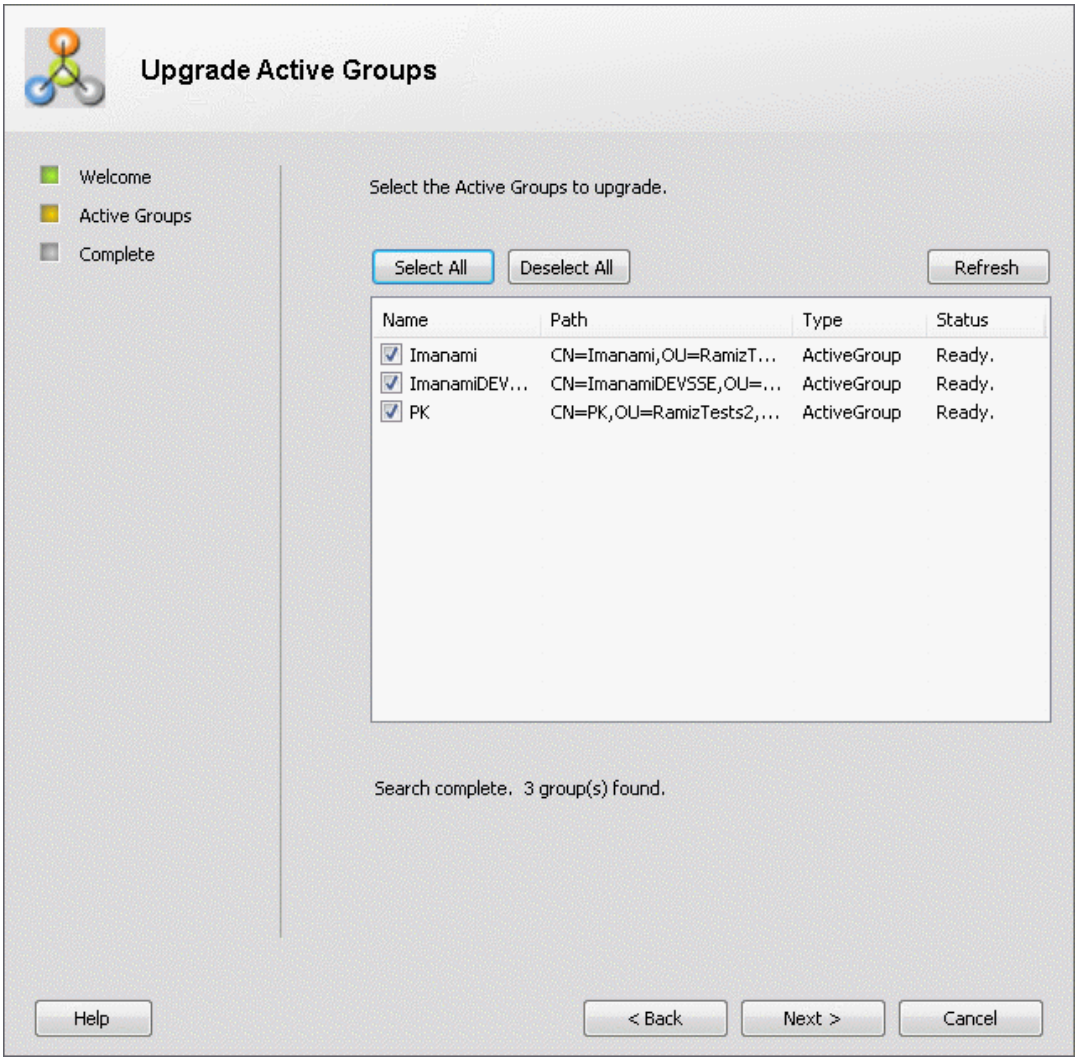


Figure - The Active Groups page

5. Once the upgrade process completes, click **Finish**.

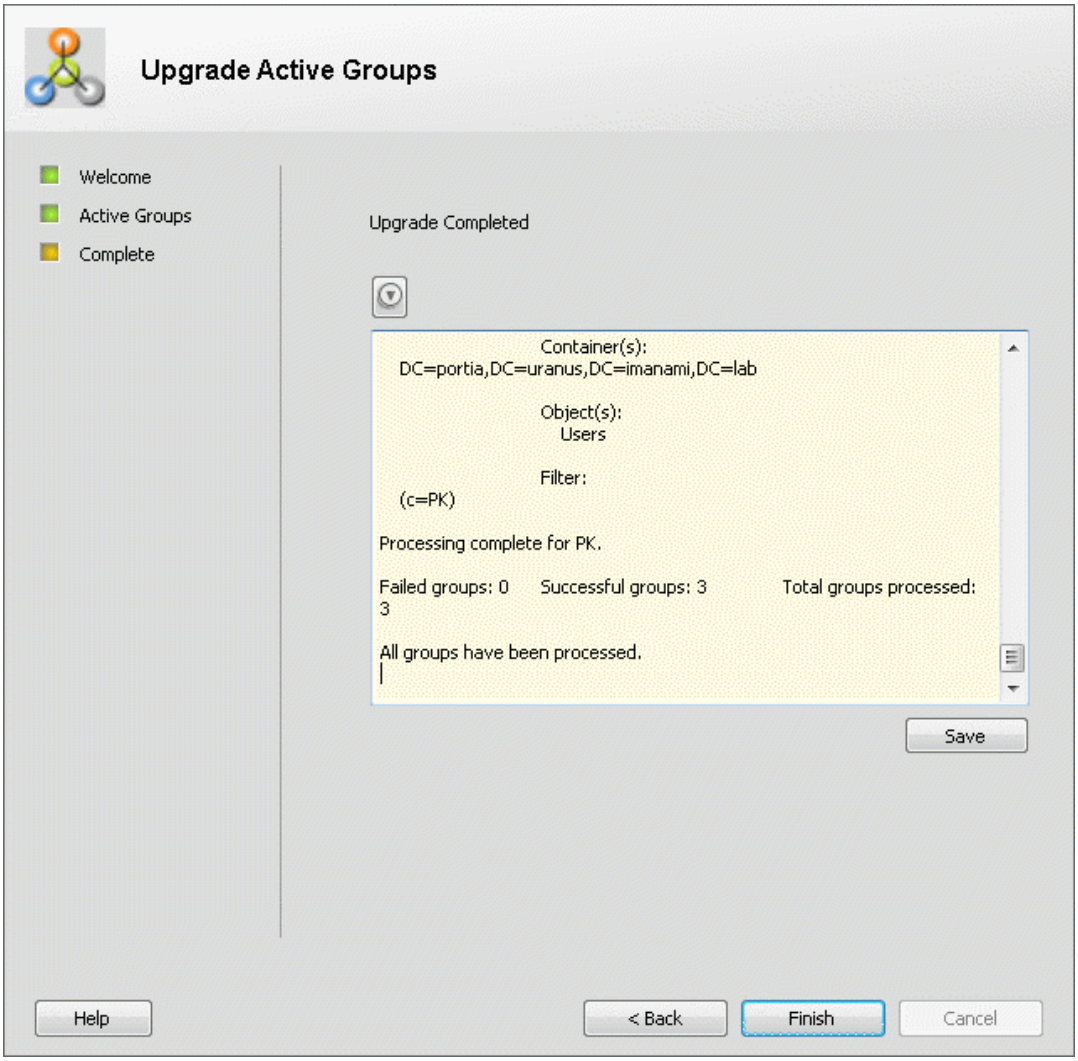


Figure - The Upgrade Completed page

Once the process completes, the wizard reports all the successfully and unsuccessfully upgraded groups.

Chapter 9: Managing Groups

A group is a collection of user and computer accounts, contacts and other groups that can be managed as a single unit. Automate classifies groups into different categories and provides comprehensive management of these accordingly. This chapter focuses on group management. The information is divided into the following:

Creating a new Group, provides instructions on creating new unmanaged groups.

Creating a new SmartGroup, provides instructions on creating new managed groups.

Updating Groups, explains different methods to update the membership of SmartGroups.

Scheduling, describes how you can define a schedule and apply it to multiple groups and containers.

Automate, explains how you can run a scheduled job using the Windows command prompt.

Moving, explains how you can move groups to other containers.

Manage Group, provides instructions on managing the primary and additional owners for groups.

Group, explains the concepts of the group expiration and renewal process. Also, it will walk you through modifying different expiry group settings.

Deleting Groups, explains how groups are deleted in Automate and provides the instructions.

Deletion, covers the information about how to configure settings for automatic deletion of expired groups.

Recycle Bin, explains when groups are moved to recycle bin and how to restore them.

Group, provides information on viewing group's history.

Group, explains the functionality of the Group Management Service.

Creating a new Group

Before creating a new group, you are required to be familiar with the following concepts:

- Group Classification
- Group Scope
- Group Type
- Group Security

The information about all these concepts is provided in **Chapter 2: Group**. After reviewing the above concepts, use the following instructions to create a new group:

1. Expand the **Automate** node, right-click **All Groups**, point to **New** and then click **Group**.
2. On the welcome page of the **New Group** wizard, read the welcome message and click **Next**.

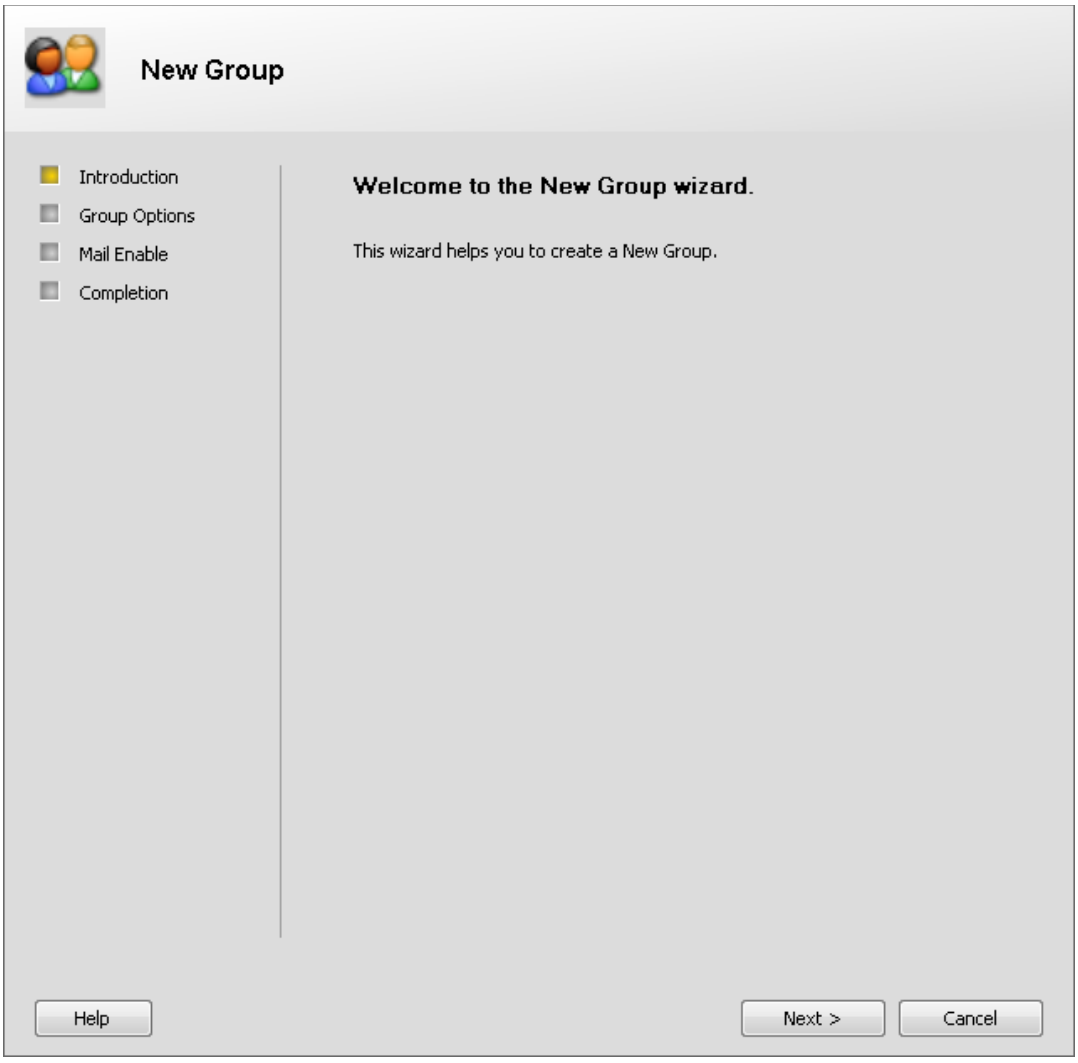


Figure - Welcome page

3. On the **Group Options** page:

i. Click **Create in**. This displays the **Browse for Container** dialog box. On the dialog box:

   a. Expand the required domain until you reach the container where you want to create the group.

   b. Click the container to select it, and then click **OK** to close the dialog box.

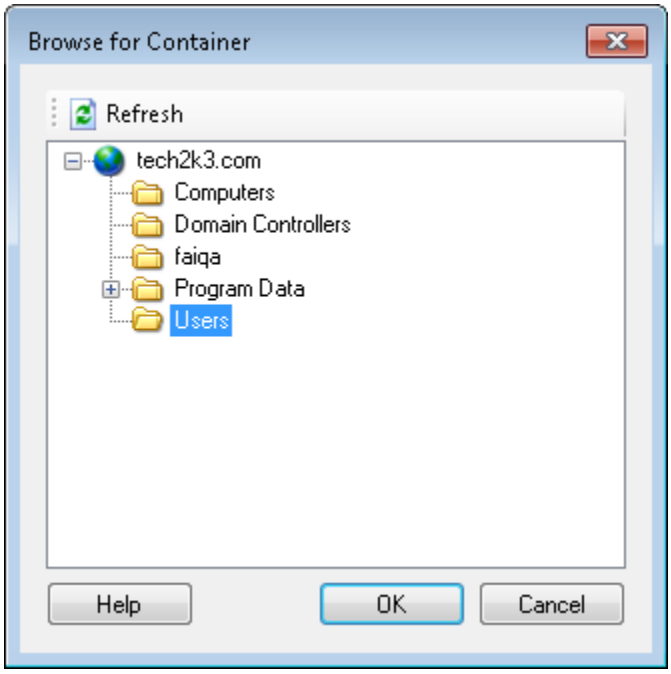


Figure - The Browse for Container dialog box

Domain selection is only allowed for unmanaged groups. SmartGroups and Dynasties can only be created in the logged on domain.

ii. In the **Group name** box, type the name of your group.
Your typed Group name is set by default for the **Group name (Pre-Windows 2000)** box. However, you can change this if required.

If prefixes are defined, the prefix list appears before the box from where you can select a prefix for the group. For information about prefixes, see **Group Name Prefixes** in **Part 7: GroupID Configurations**. After selecting the prefix; as you type the Group name, it shows the **Name Preview** including the prefix, below the box.

Figure - The prefixes list

iii. In the **Group Scope** area, select the required scope for the group. For information about group scope, see **Group Scope** in **Chapter 2: Group Management Concepts**.

iv. In the **Group Type** area, select the required type. For information about group types, see **Group Types** in **Chapter 2: Group Management Concepts**.

v. From the **Group Security** list, select the required security type. For information about security types, see **Security Type** in **Chapter 2: Group Management Concepts**.

Requires Self-Service license

vi. Click **Next**.

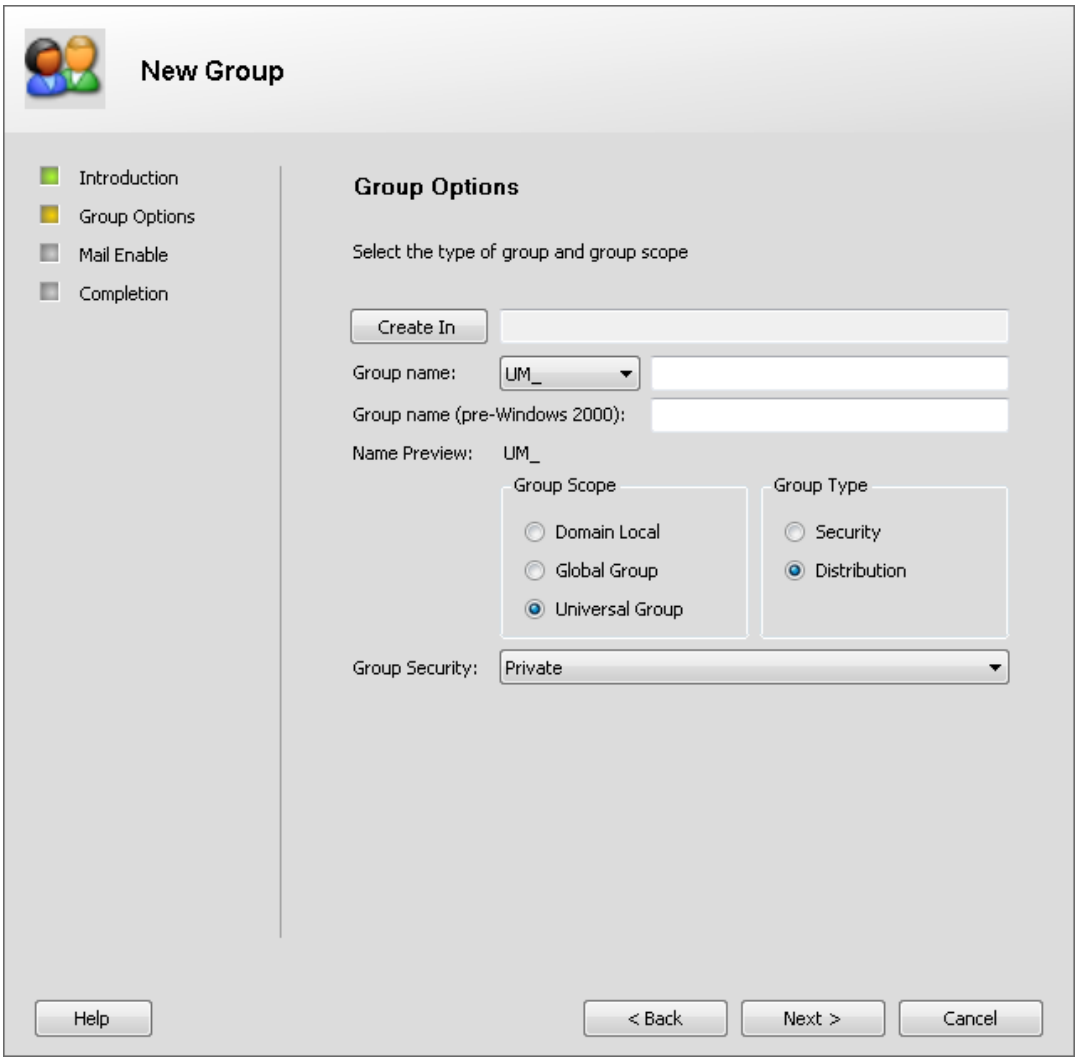


Figure - Group Options page

4. Skip this page if you do not want to mail-enable your Group. On the **Mail-enable Group** page:

i. Select the **Create an Exchange e-mail address** check box, if not already selected, to make this new group a mail-enabled group.

ii. In the **Alias** box, type an alias for this group. Normally, the alias is copied from what is typed in the **Name** field.

iii. Click **Next**.

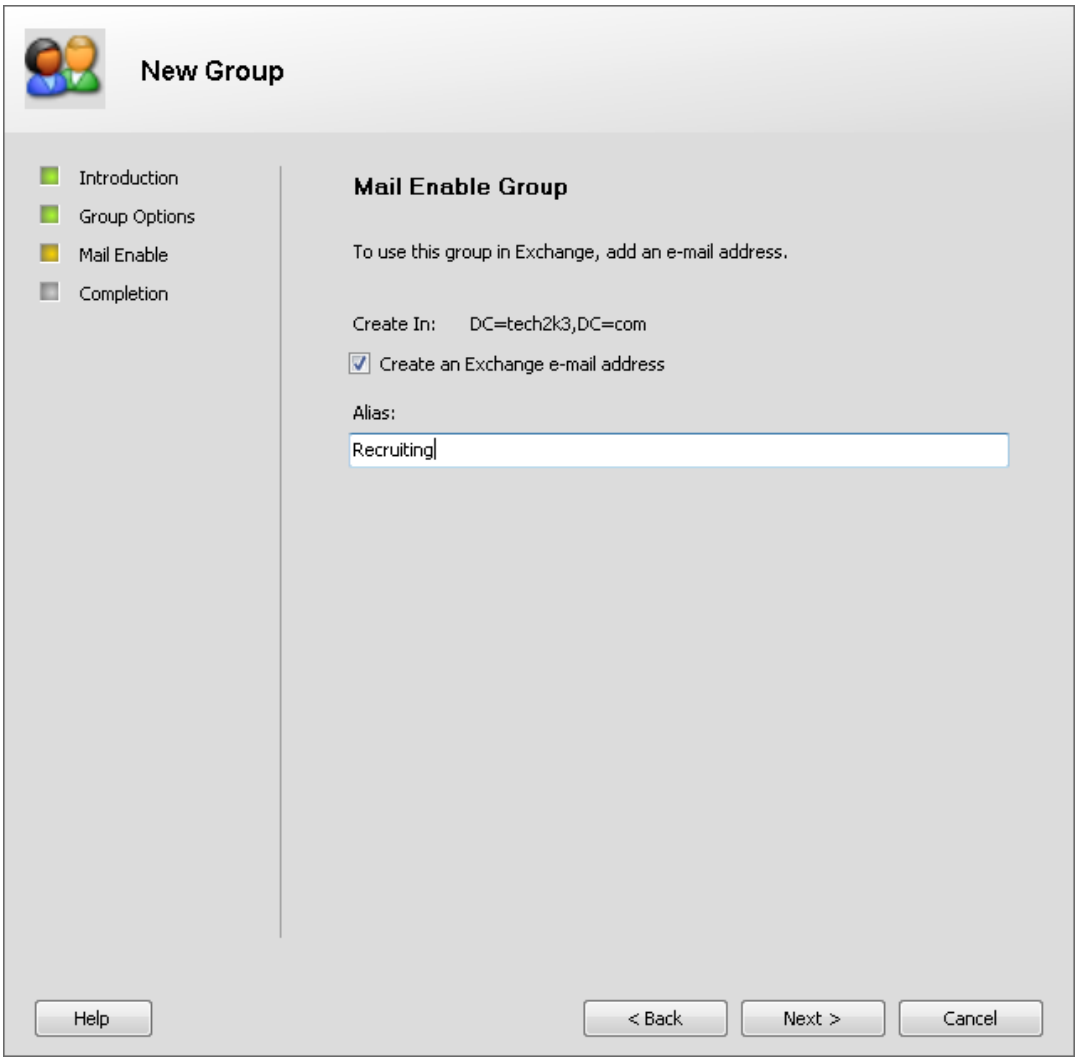


Figure - Mail-enable Group page

5. On the last page of the wizard, click **Finish** and then click **Close** to create the new group.

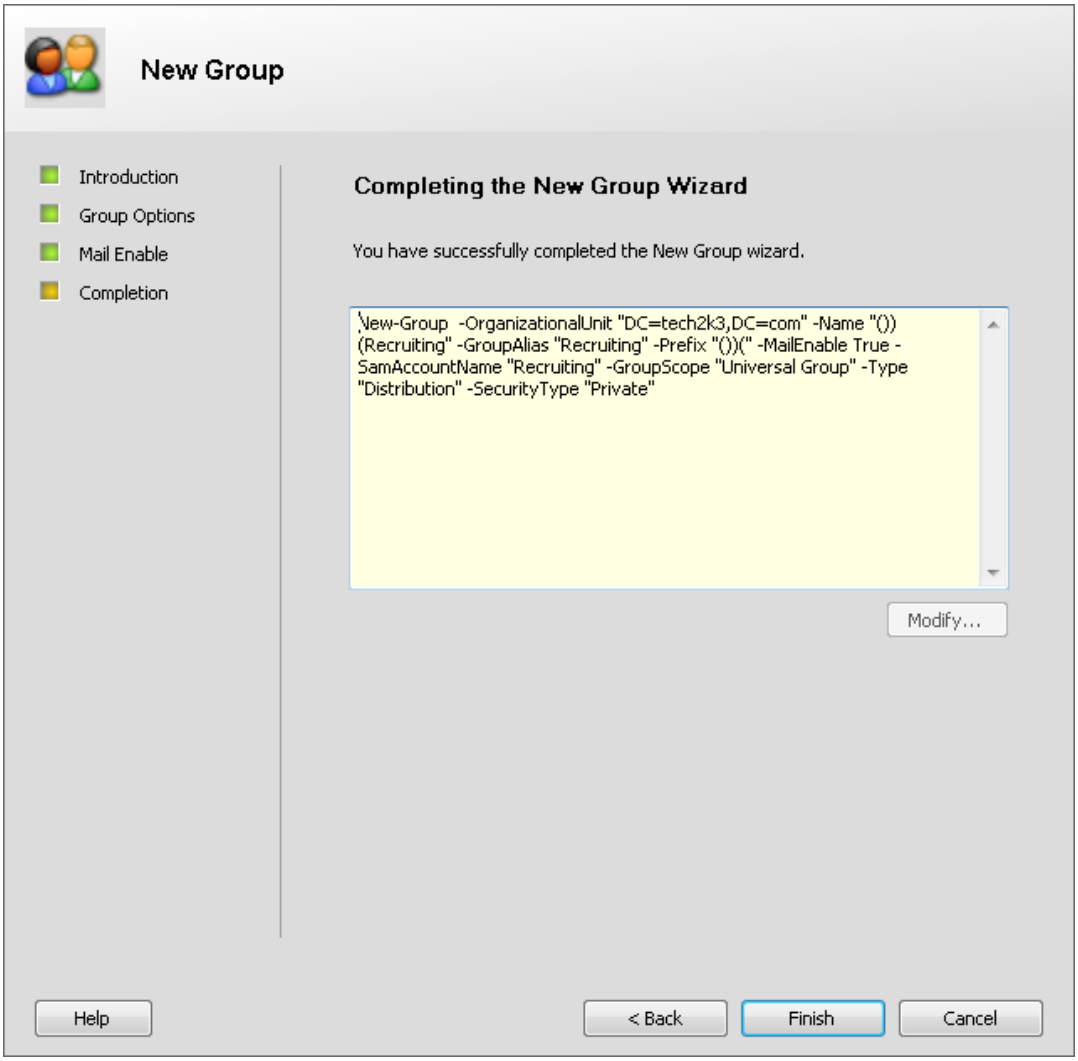


Figure - Completing the New Group Wizard page

Creating a new SmartGroup

A SmartGroup is one that dynamically maintains its membership based on the rules applied by a user-defined LDAP query. For more information about SmartGroups, see **Group** in **Chapter 2: Group Management Concepts**. A SmartGroup can also be defined as a **Password Expiry group**. A Password Expiry group is a dynamic group whose membership is based on password policy conditions defined by the administrator. Members of this group receive notification to reset their password after a specific number of days in order to be removed from the group membership.

> To create password expiry groups, you must have a password policy defined within the local security policy for your domain or domain controller.

The instructions below guide you on how to create a new SmartGroup:

1. Expand the **Automate** node, right-click **All Groups**, point to **New** and then click **SmartGroup**.

2. On the welcome page, select either:

- **Run to create SmartGroup**, to create a new SmartGroup.
- **Run to create Password Expiry group**, to create a Password Expiry group.

3. Click **Next**.

Figure - The Welcome page

4. On the **Group Options** page:

   i. Click **Create in** to select the container in which to create the new group.

   ii. In the **Group name** box, type the name of your group.
   Your typed Group name is set by default for the **Group name (Pre-Windows 2000)** box. However, you can change this if required.

If prefixes are defined, prefixes list appears before the box from where you can select a prefix for the group. For information about prefixes, see **Group Name Prefixes** in **Part 7: GroupID Configurations**. After selecting the prefix; as you type the Group name, it shows the **Name Preview** including the prefix, below the box.

Figure - The prefixes list

iii. From the **Group Scope** area, select the required scope for the dynasty. For information about group scope, see **Group Scope** in **Chapter 2: Group Management Concepts**.

iv. From the **Group Type** area, select the required type. For information about group types, see **Group Types** in **Chapter 2: Group Management Concepts**.

v. From the **Group Security** list, select the required security type. For information about security types, see **Security Type** in **Chapter 2: Group Management Concepts**.

Requires Self-Service license

vi. Click **Next**.

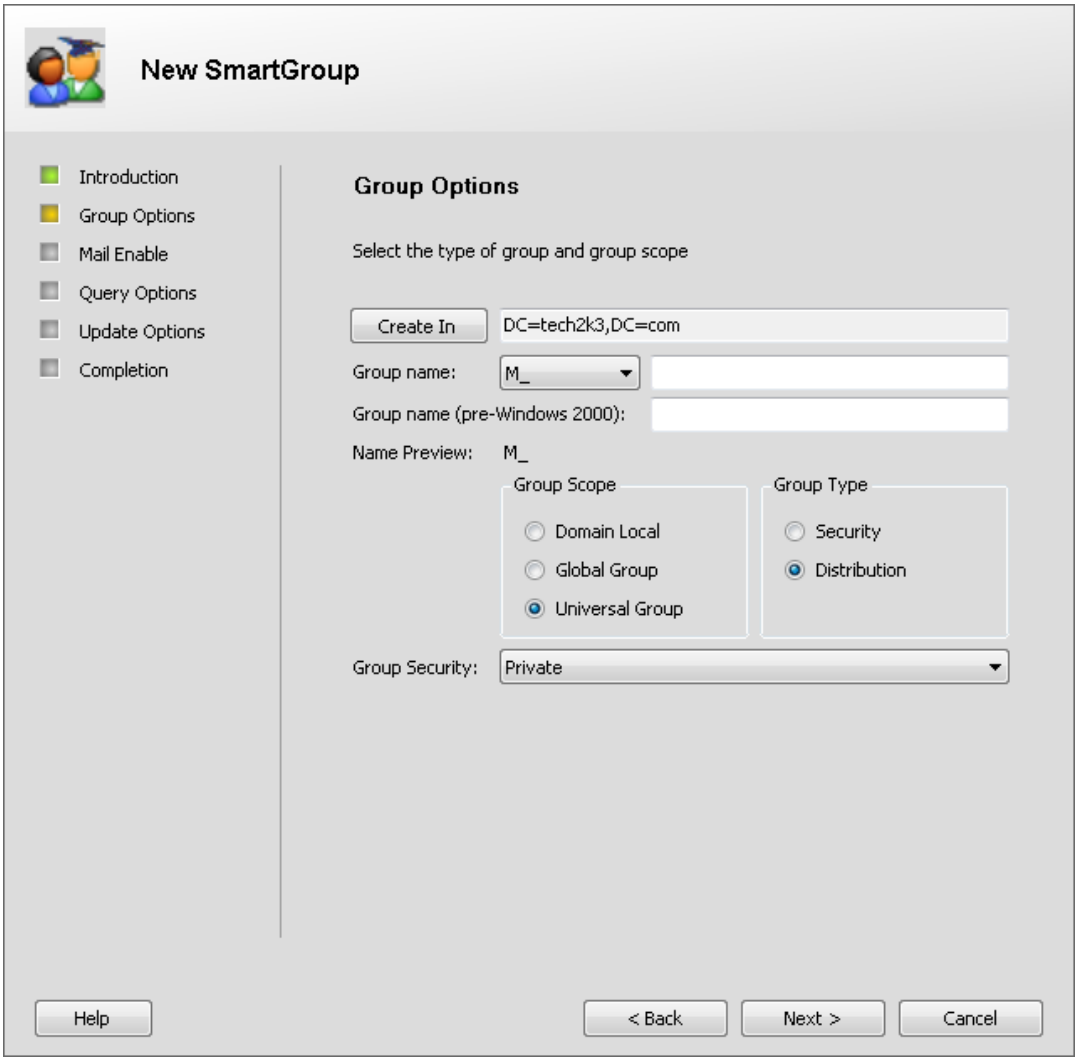


Figure - The Group Options page

5. Skip this page if you do not want to mail-enable your SmartGroup. On the **Mail-enable Group** page:

    i. Select the **Create an Exchange e-mail address** check box, if not already selected, to make this new group a mail-enabled group.

    ii. In the **Alias** box, type an alias for this group.

    iii. Click **Next**.

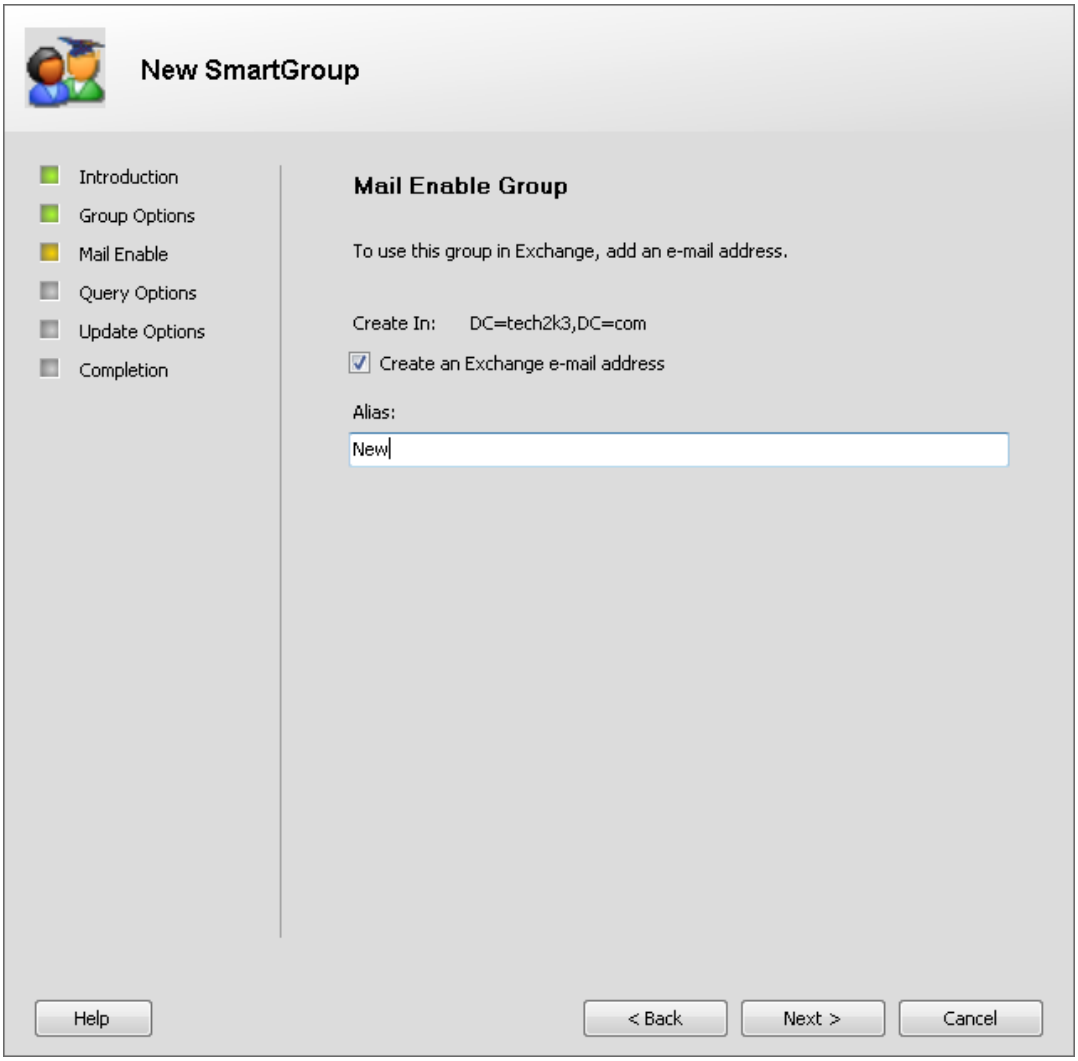


Figure - The Mail-enable Group page

6. The **Query Options** page shows the default query for selecting the group members. The default query returns all users and contacts in the container, which are then grouped by the specified attributes.
   You can click **Modify** to launch the **Query Designer** where you can edit the query. For detailed information about the query designer, **Chapter 13: The Query Designer**.

7. Click **Next**.

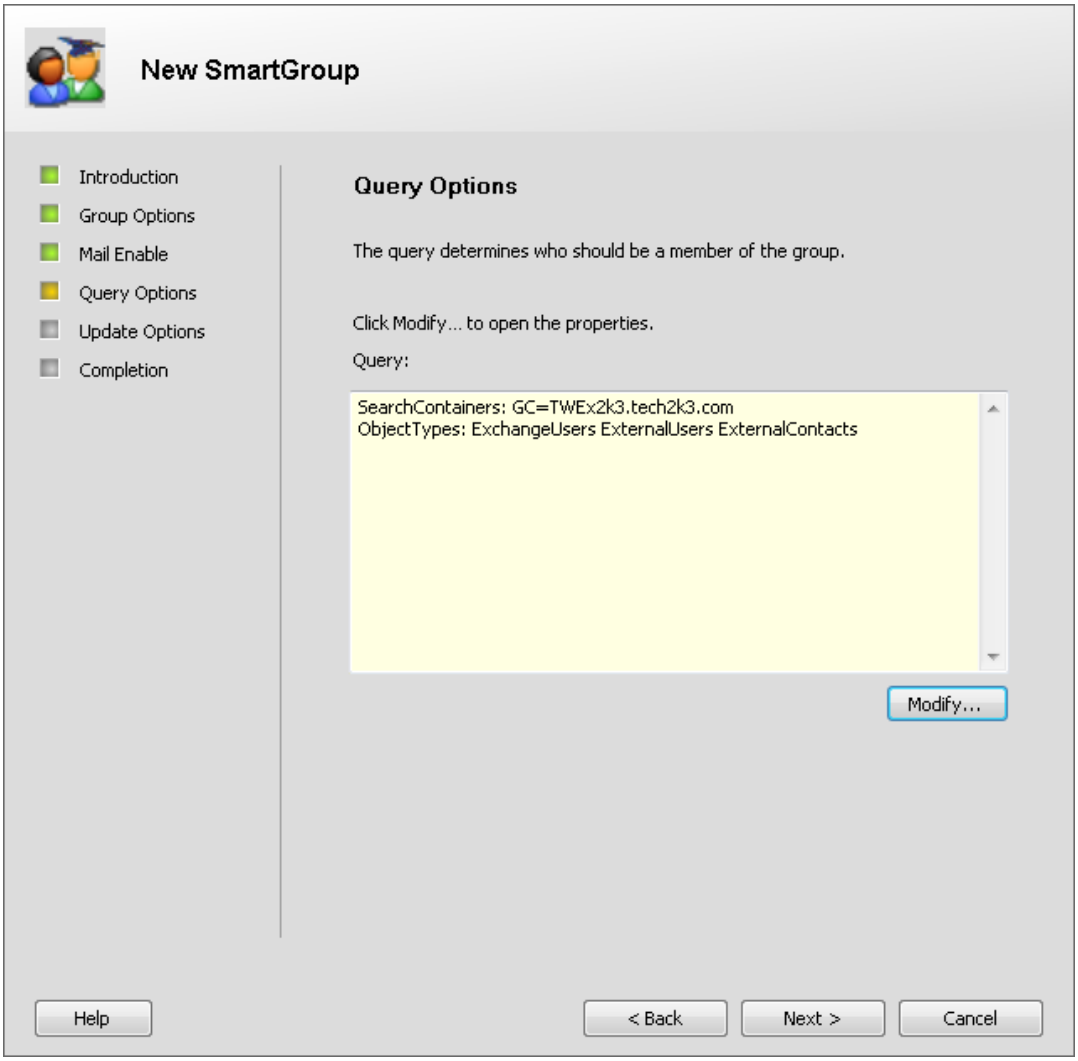


Figure - The Query Options page

8. On the **Update Options** page, select when you want to update the group memberships. Following options are available:

    - **Now**, to update the group membership as soon as you click **Next**.
    - **Later, using the Update command or an existing job**, to manually update the group membership later. This can be done by right-clicking the group in the groups list and clicking **Update**. You can also apply a job schedule to the group later, if required.
    - **Later, using a new job on this machine**, to create a job schedule to update the group membership. You provide the frequency (daily, weekly, monthly and so on) and timings for the job schedule and it automatically updates the group memberships according to the defined schedule.

9. Click **Next**.

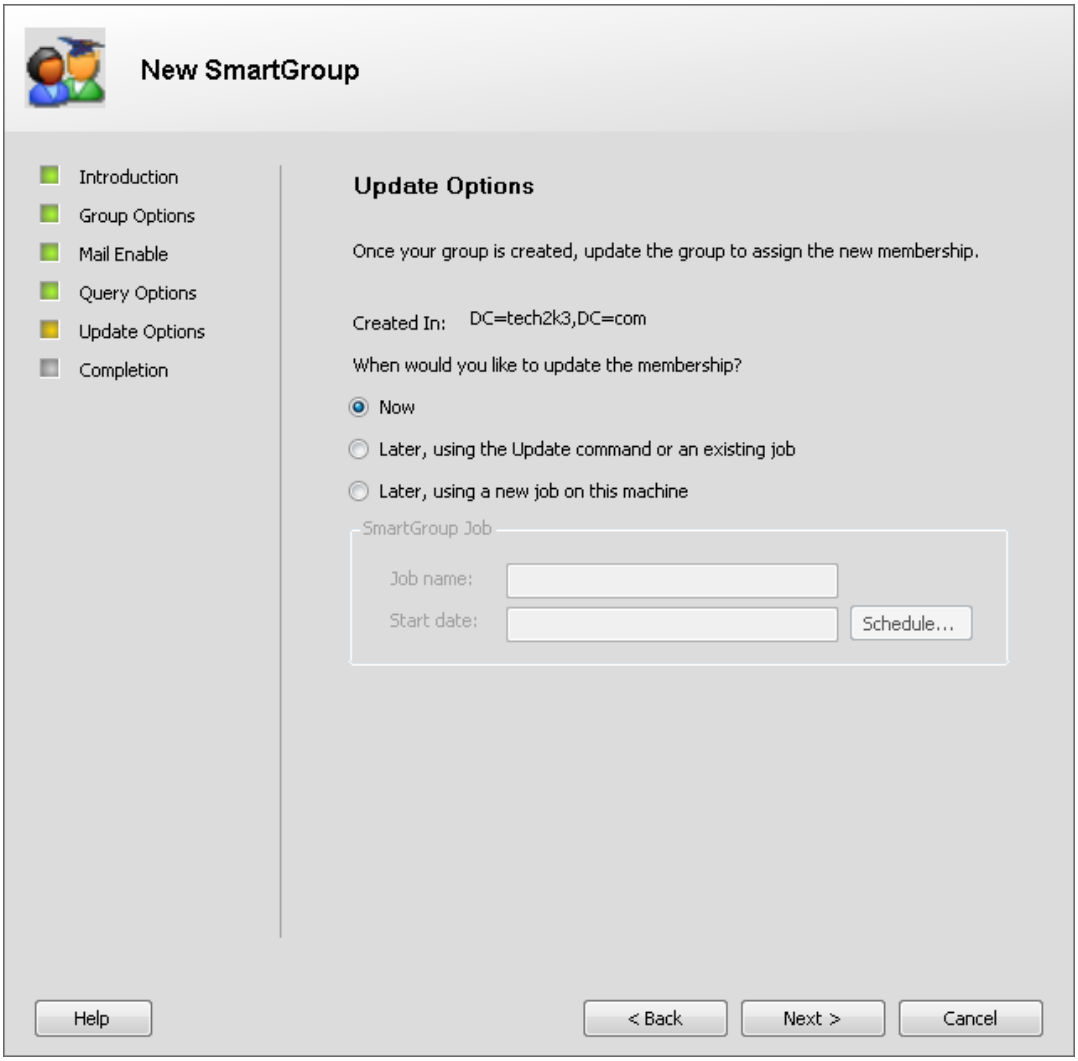


Figure - The Update Options page

10. On the last page of the wizard, click **Finish** to create the new SmartGroup.

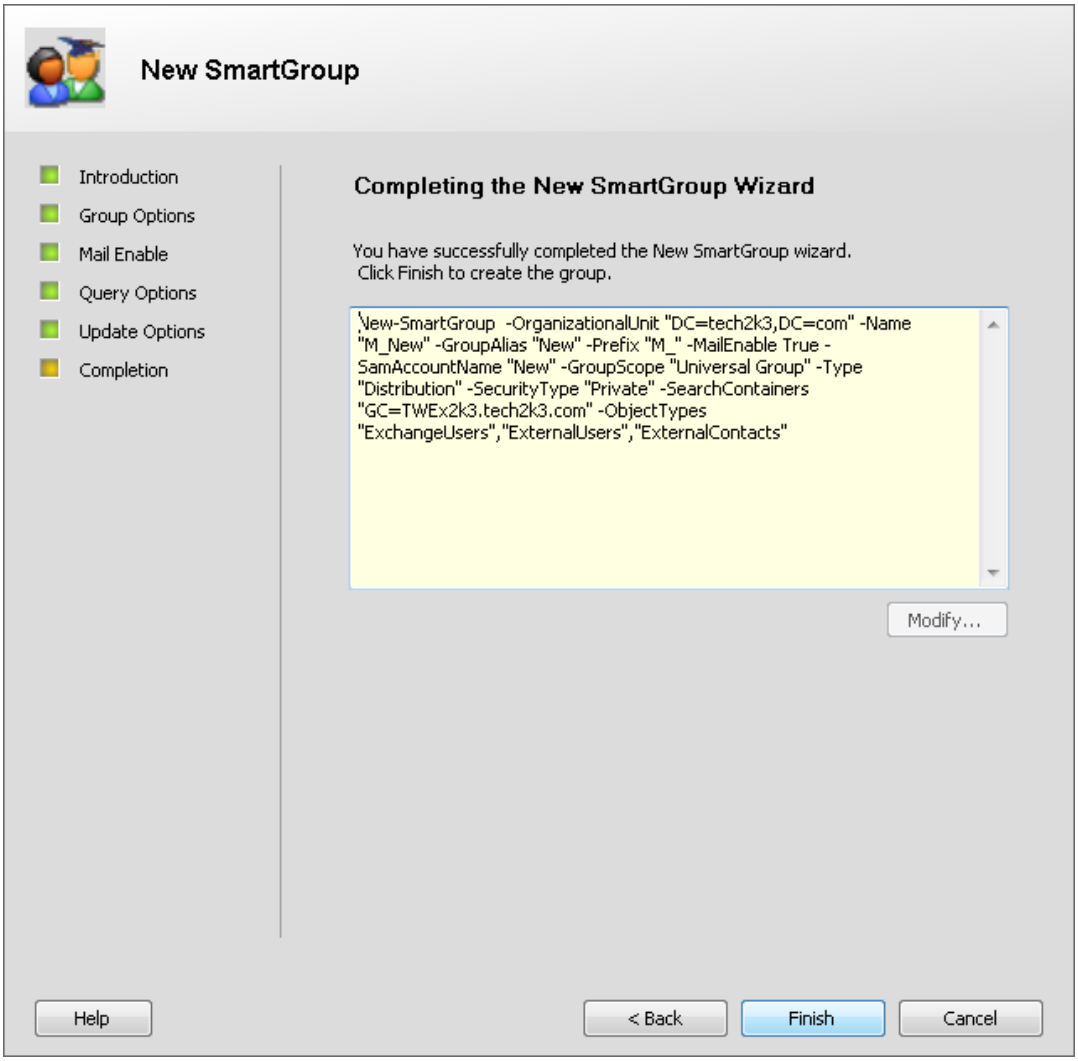


Figure - Completing the New SmartGroup Wizard

Updating Groups

One of the main features of Automate is to dynamically update the memberships of SmartGroups based on user-defined queries. These queries are defined once and you can execute them to update the group memberships as soon as there is a change in your Active Directory.

Automate provides different methods to update SmartGroup memberships which are as follows:

1. **While creating a SmartGroup**

   During the creation of a SmartGroup, the **Update Options** page of the **New SmartGroup** wizard provides you an option to immediately update the group memberships based on the given query. Selecting the option adds members to the group as it is created.

2. **Using a new job schedule**

The **Update Options** page of the **New SmartGroup** wizard provides another option to define a new job schedule for updating memberships. Selecting the option lets you define a schedule which describes the frequency, date and time when the query will execute the update of group membership. For more information about job schedules, see **Scheduling** later in this chapter.

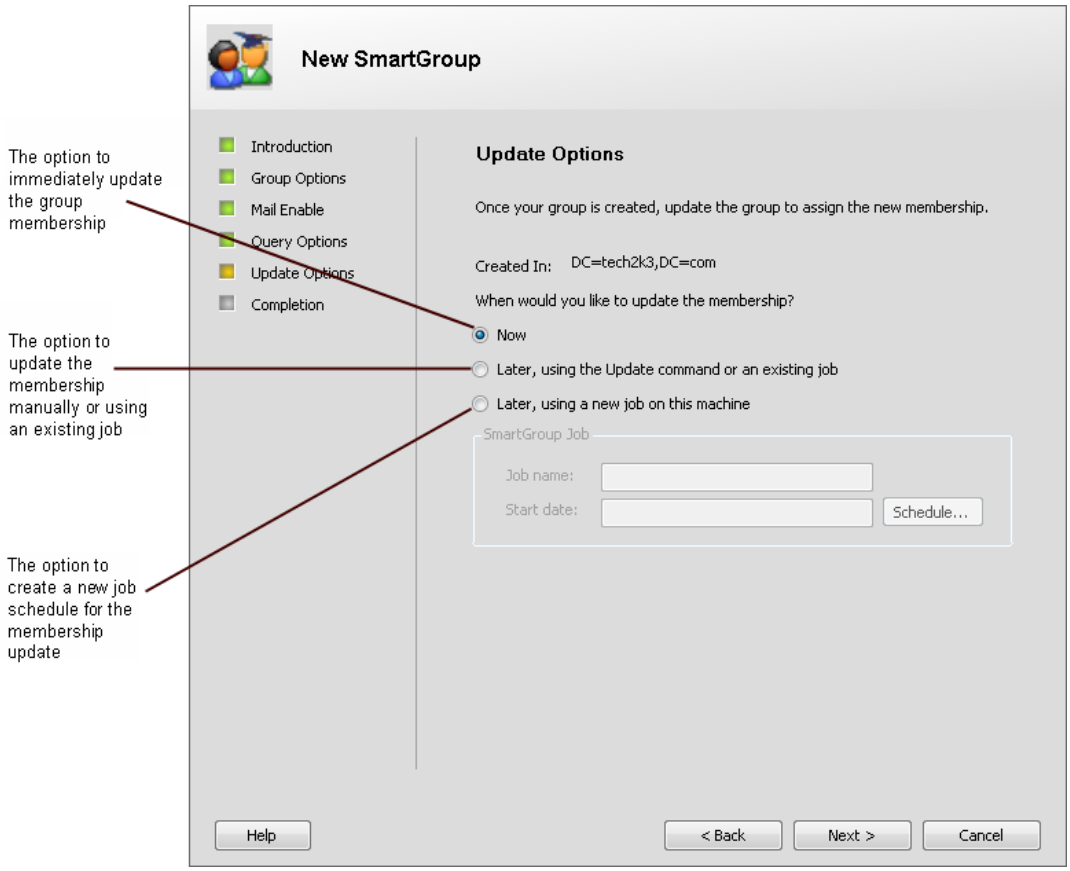

The option to immediately update the group membership
The option to update the membership manually or using an existing job
The option to create a new job schedule for the membership update
New SmartGroup
Introduction
Group Options
Mail Enable
Query Options
Update Options
Completion
Update Options
Once your group is created, update the group to assign the new membership.
Created In: DC=tech2k3,DC=com
When would you like to update the membership?
Now
Later, using the Update command or an existing job
Later, using a new job on this machine
SmartGroup Job
Job name:
Start date:
Schedule...
Help
< Back
Next >
Cancel

Figure - The Update Options page

3. Using an existing job schedule

If you already have a job schedule defined, you can add the group to the targets list of the job. For information about the targets list, see **Scheduling** later in this chapter.

4. Manual Update

You can manually run the update membership query for one or more SmartGroups any time by right-clicking the groups after selection and clicking **Update** on the shortcut menu. This will execute the query immediately for each selected group to update its membership.

To select multiple groups, hold down the **CTRL** key and select individual groups or hold down the **SHIFT** key and select a range of groups.

Scheduling Jobs

Scheduling a job will help to automatically update the memberships of SmartGroups and Dynasties on an ongoing basis. For detailed information about Dynasties, see **Chapter 12: Dynasties**. You need to create the job once and the Group Management Service running in the background will update the group membership as per the schedule. A job is composed of the following items:

	Job Item	Description
1.	Schedule	A schedule defines the frequency, date and time when the job will execute to update the membership. For example, you can schedule a job to run Daily at 10:00 AM starting from the date January 01, 2009 to December 31, 2009.
2.	Targets list	This list contains groups and containers that will be processed by the job.
3.	Credentials	A job requires credentials to connect to the domain and update group memberships.
4.	Notification	A job can be configured to send a summary report to the administrator and the group owner when it completes the update operation.

There are two ways using which you can schedule jobs in Automate:

- **Using group Properties dialog box**

  The **Schedule** button is available from the **GroupID** tab of the Properties dialog box for SmartGroups and Dynasties. This feature sets a schedule based on the individual group or dynasty. To set a schedule for an entire container or domain, please review **Using the Scheduling dialog box** in this section.

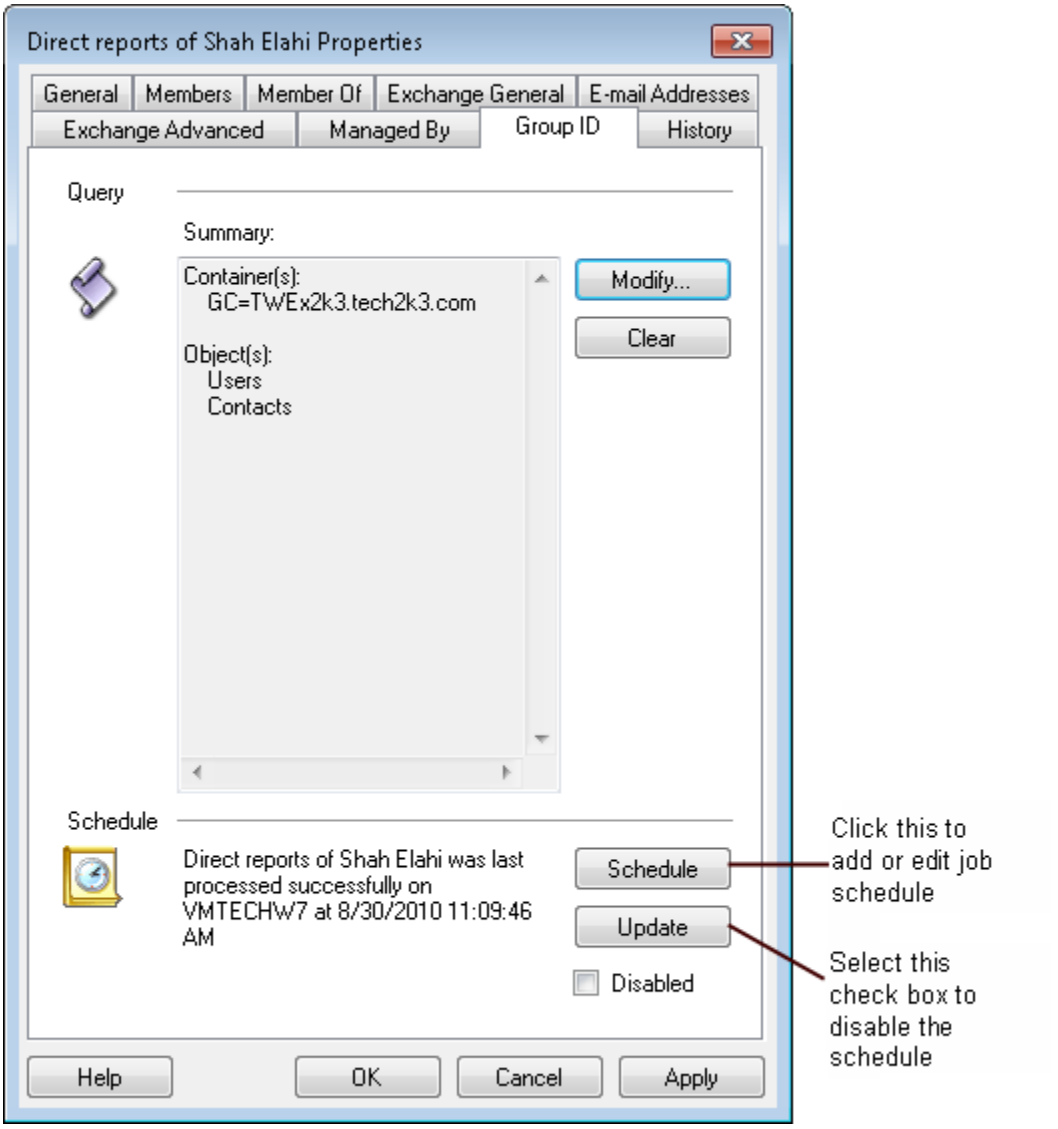


Figure - The Schedule button on the GroupID tab

- **Using the Scheduling dialog box**

  The scheduling setting is available when you right-click the **All Groups** node and click **Scheduling**.

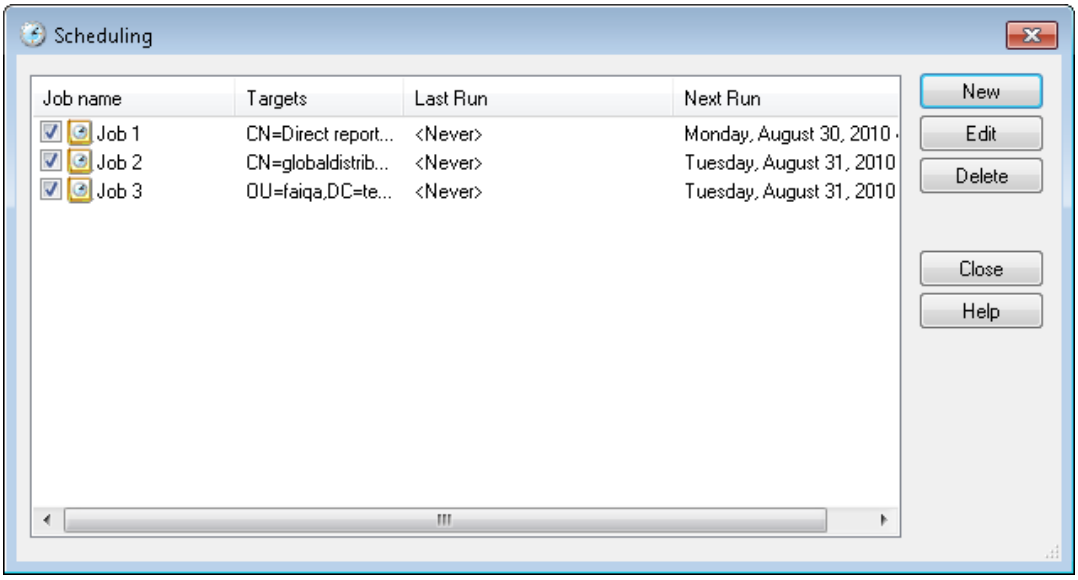


Figure - The Scheduling dialog box

Creating a Scheduled Job

1. On the Edit Job dialog box, provide the following information:

    i. In the **Job Name** box, type the name of the job. By default, the box displays a system suggested job name. You can use this name as it is for the job.

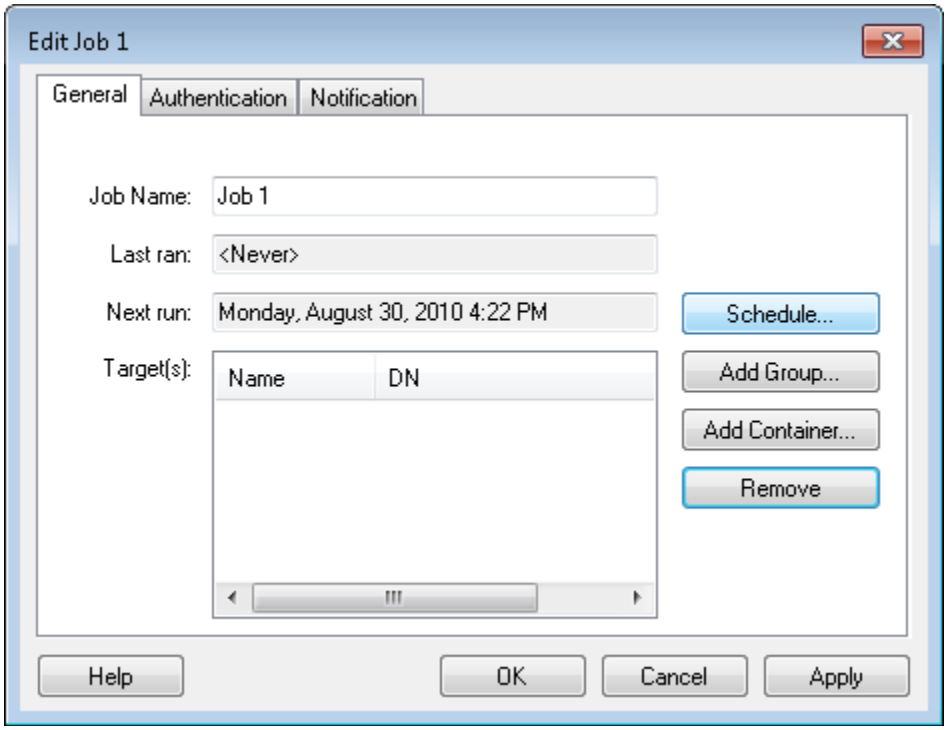


Figure - The Edit Job dialog box

    ii. Click **Schedule**. This displays a dialog box where you can define the date, time, frequency and other preferences for the schedule.

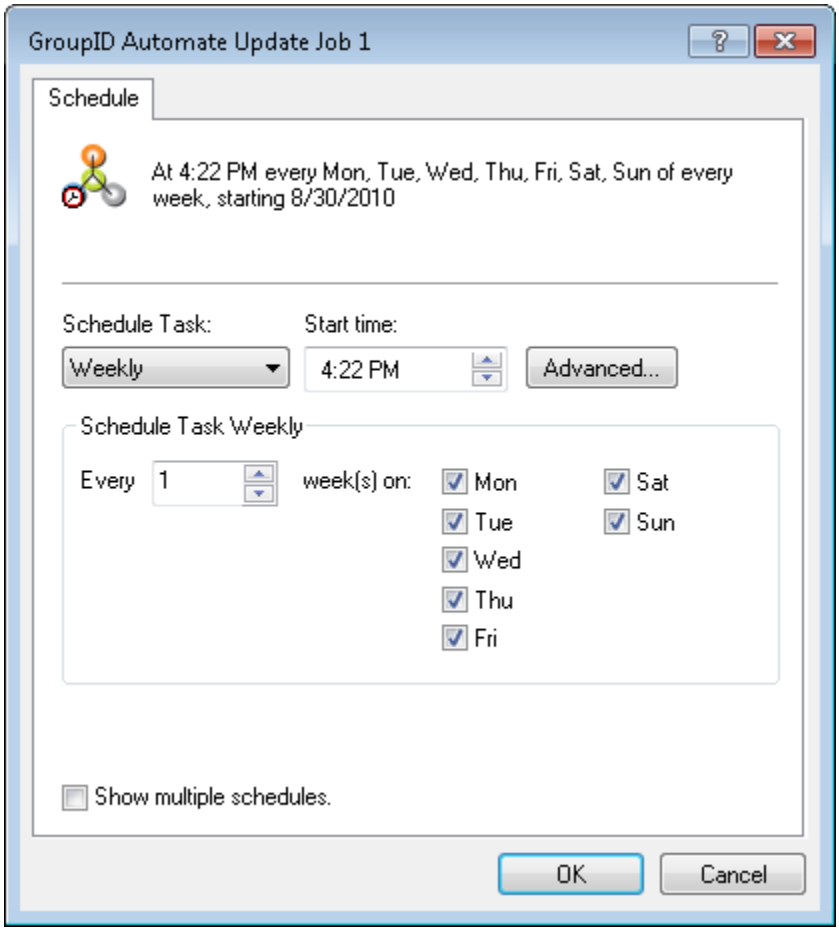


Figure - The dialog box for defining the job schedule

iii. The **Target(s)** list shows the containers and/or groups for which the job is scheduled to update. You can add more groups and containers in the list, if required.

- To add groups, click **Add Group**. This displays the **Find Groups** dialog box where you can find and select the required groups.
- To add containers, click **Add Container**. This displays the **Select Container** dialog box where you can select the required container within the Active Directory tree.

You can remove a group or container from the **Target(s)** list by selecting it, and then clicking **Remove**.

2. Click **OK** to close the Edit Job dialog box.

Adding notification

1. On the Edit Job dialog box, click the **Notification** tab and use the following instructions to add notification:

   i. Select the **Send a job completion report** check box. This makes the **Options** section available to modify the notification settings.

ii. In the **To** box, type the e-mail address whom you want to send the notification.

a. Select the **Send report to group owner(s)** check box if you want to notify the group owner.

b. From the **Send Report When** area, select any of the following options as required:

- **Always send report**, to always send the notification whether the job succeeds or fails.
- **Only when job succeeds**, to send the notification only if the job succeeds.
- **Only when the job fails**, to send the notification only if the job fails.

Click **OK** to close the Edit Job dialog box.

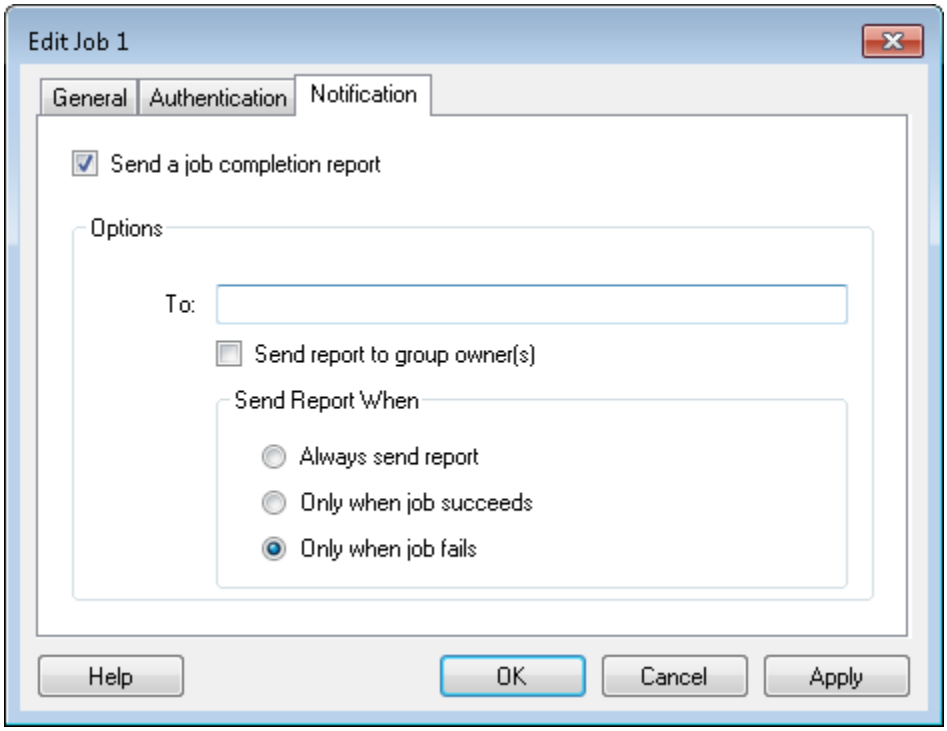


Figure - The Notification tab

Automate Command-line Utility

The command-line utility for Automate is designed to facilitate executing scheduled jobs to update group memberships instantaneously instead of waiting for the next job run according to its schedule. For more information about scheduled jobs, see **Scheduling** earlier in this chapter. You can use this utility from Windows command prompt to run the job.

Automate command-line utility is available in the installation directory for GroupID by the name **Imanami.GroupID.Automate.exe**.

To run a job using this command-line utility:

1. On the command prompt, move to the installation directory for GroupID. By default, GroupID is installed to the location: **C:\Program Files\Imanami\GroupID**.

2. Type the following command:

```
Imanami.GroupID.Automate "Job Name"
```

3. Press **Enter** to run the command. This will show the targets (groups and/or containers) that the job will process and update their membership, if changes are found in the Active Directory data.

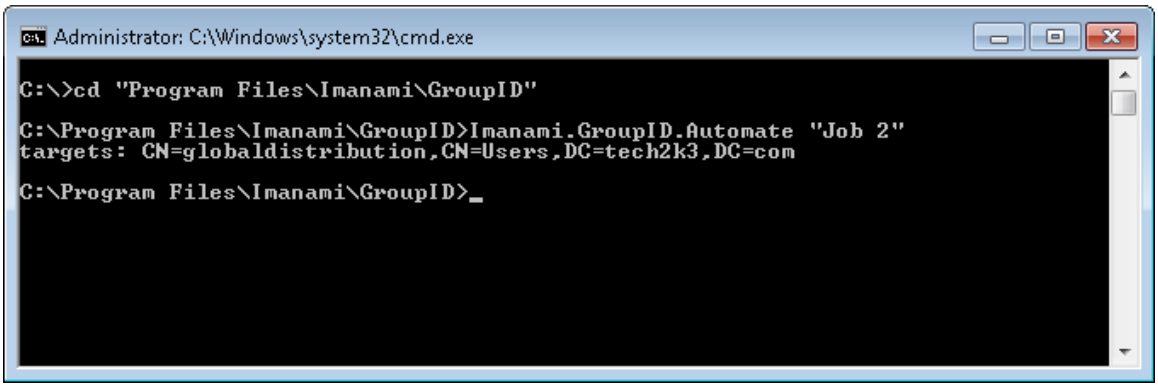


Figure - the command prompt showing the job details

Moving Groups

You can move groups from one container or organizational unit to the other. The destination container can exist on the same domain or a different domain that is a part of the same forest.

To move groups:

1. Expand the **Automate** node and select the required group node.

2. From the groups list, select one or more groups as required:

   - To select consecutive groups; click the first group in the list, press and hold down the **SHIFT** key and then click the last group.

   - To select non-consecutive groups, press and hold down the **CTRL** key and then click each group that you want to select.

3. Right-click the selection and then click **Move**. This displays the **Select Container** dialog box where you can select the required container.
   If you want to move groups to a different domain, click **Server**. This displays the **Connect to Domain** dialog box where you can provide credential for connecting to the domain. If valid credentials are provided, the containers list is refreshed on the **Select Container** dialog box showing the containers of the selected domain. Here you can select the required container.

4. Click **OK** to close the **Select Container** dialog box.

Manage Group Owners

When a new group is created; by default, the group creator is set as its primary owner. However, the administrator and the primary owner have the privileges to set a different recipient as the group owner, if required. They also have permissions to set additional owners for the group for receiving groups expiry and deletion notifications on which they can respond when the primary owner is out of office.

Change primary owner for groups

To change primary owner for a group, follow the instructions below:

1. Expand the **Automate** node and select the required group node.
2. From the groups list, right-click the required group and then click **Properties**.
   This displays the Properties dialog box for the selected group.
3. On the **Managed By** tab, click **Change**.
   This displays the **Find** dialog box.
4. Use the **Find** dialog box to search and select the recipient you want to set as the primary owner for the group.
5. Click **OK** to close the Properties dialog box.

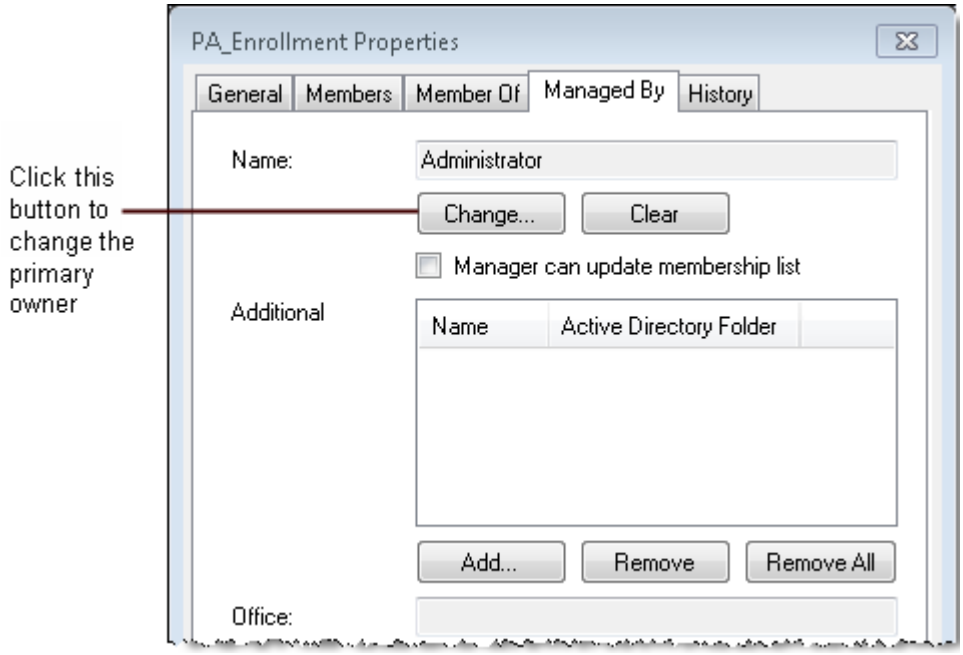


Figure - Change button on the Managed By tab

To change primary owner for multiple groups collectively, follow the instructions below:

1. Expand the **Automate** node and select the required group node.
2. From the groups list, select required groups using any of the following methods:
   - To select consecutive groups; click the first group in the list, press and hold down the **SHIFT** key and then click the last group.

- To select non-consecutive groups; press and hold down the **CTRL** key and then click each group that you want to select.

3. Right-click the selected groups, point to **Set Owner** and click:

   - **Me [*your logged on user name*]**, to set yourself as the primary owner for selected groups.
   - ***Most recently used recipient set as primary owner (if any)***, to set this recipient as the primary owner for selected groups.
   - **Other...**, to select a different recipient as the primary owner. Clicking this option displays the **Set Owner** dialog box where you can find and select the recipient you want to set as the primary owner for selected groups.

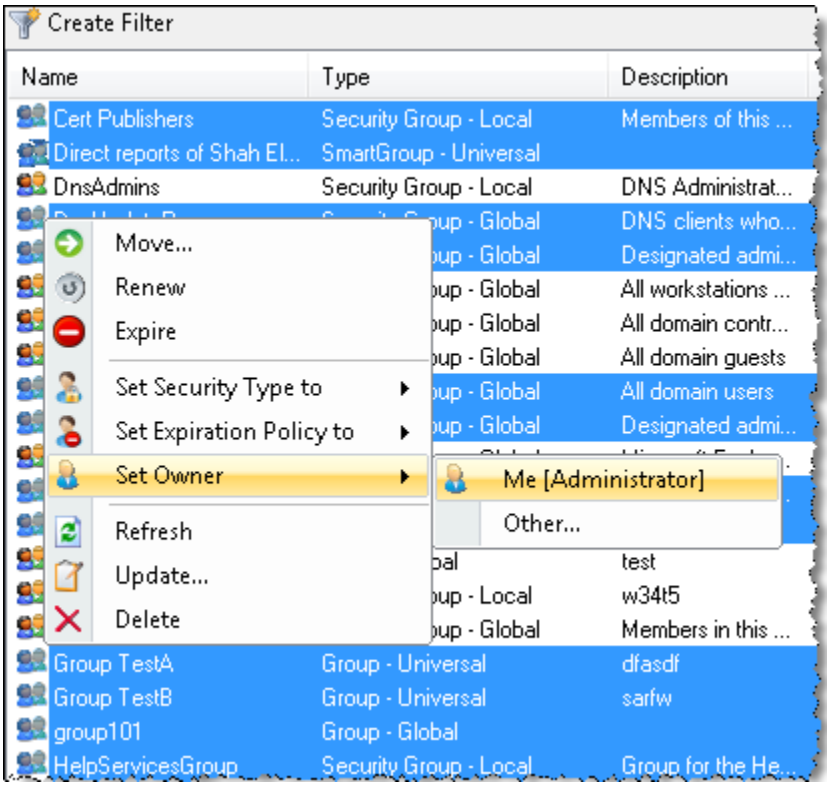


Figure - Set Owner command on the shortcut menu

Set additional owners for a group

The option for setting additional owners is available right below the primary owner on the **Managed By** tab. For the domains with Exchange Server 2010 deployed, additional owners can also be added using the **Exchange General** tab. In this case, group expiry and deletion notifications are sent to all additional owners - selected on Managed By tab and Exchange General tab - along with the primary owner.

To add additional owners on the **Managed By** tab:

1. Expand the **Automate** node and select the required group node.
2. From the groups list, right-click the required group and then click **Properties**.
   This displays the Properties dialog box for the selected group.

3. On the **Managed By** tab, click **Add** below the **Additional Owners** box.
   This displays the **Find** dialog box.

4. Use the **Find** dialog box to search and select the recipient you want to set as the additional owner for the group.

5. Click **OK** to close the Properties dialog box.

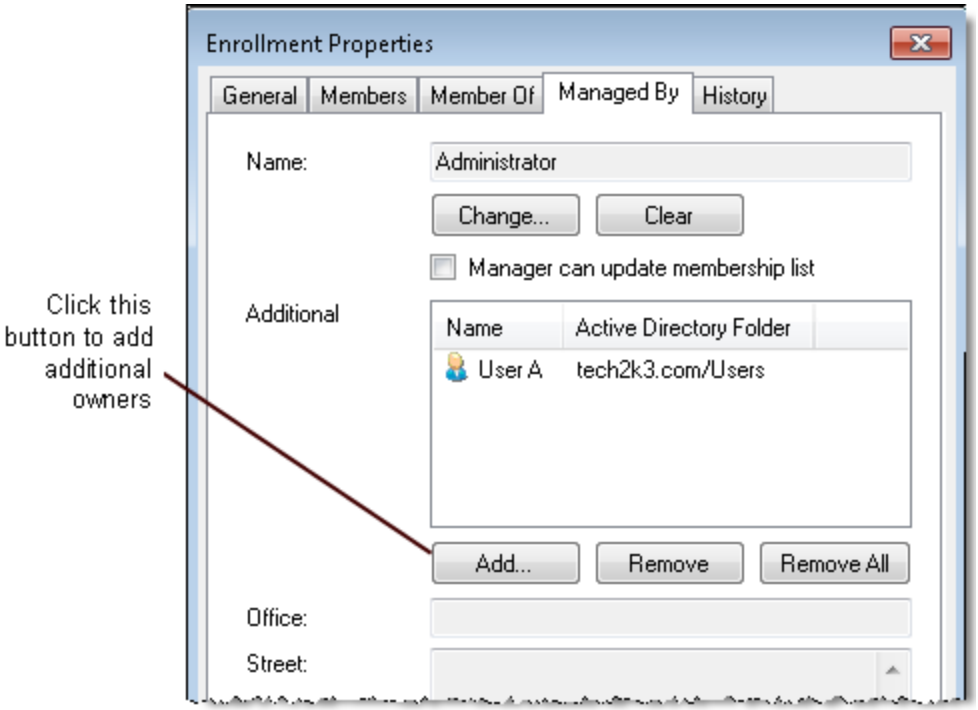


Figure - Add button on the Managed By tab

To add Exchange Server 2010 additional owners:

1. On the Group Properties dialog box, click the **Exchange General** tab.

2. In the **Managed By** area, click **Add**.
   This displays the **Find** dialog box where you can search and select the recipients you want to set as the additional owners for the group.

3. Click **OK** to close the Group Properties dialog box.

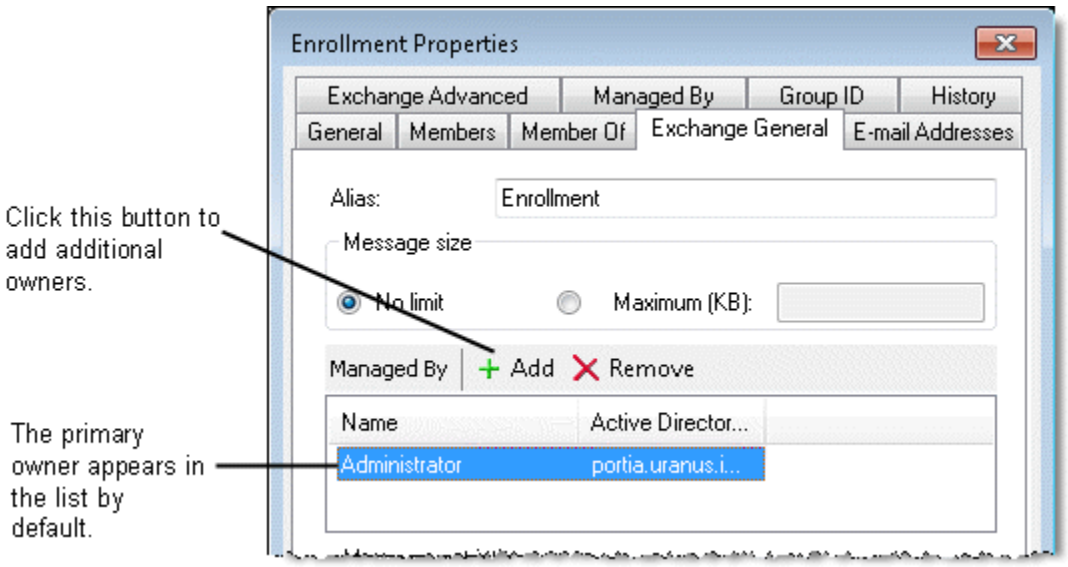


Figure - Add button on the Exchange General tab

Group Expiry

Group expiration is a key component of a group's Lifecycle. Today, many organizations complain about group glut, the proliferation of groups in the Global Address List that results in user confusion and even internal spam. Groups in Active Directory should have an end lifecycle since the need for all groups is not necessary for a life time. Some organizations have up to 8 times more groups than users due to the lack of tools for monitoring groups and their usage activities in their environment.

GroupID solves this problem by offering an automated way to expire groups cluttering the Global Address List. When you create a group, GroupID associates a default expiration policy with the group. This expiration policy is configurable using the global settings and can also be changed for each group individually. The expiration policy defines the period for which the group remains active. Group Management Service running in the background monitors the expiration policy of all groups. When a group approaches its expiry, the service notifies the owners (primary and additional owners) or the default approver (in case no owner is set for the group) about it. Sending notifications requires SMTP server to be configured properly. For information about configuring SMTP server, see **Notifications Settings** in **Part 7: GroupID Configurations**. If due to incorrect SMTP settings the notifications are not delivered to the designated recipient, the service will extend the expiration policy of the group by 7 days on the last day of its expiry. The service will continue this process and its notification attempts until the correct SMTP settings are configured. You can bypass the notifications process, if you want the service to expire groups without notifying anyone. When the expiry period of a group is over, it becomes inactive and is locked for all activities. If the expired group is a distribution group, no e-mails can be sent to it. If there is still a need for the group, getting it back is as simple as renewing it.

Requires Self-Service license

Expiring Groups

An expiration policy defines the period for which the group remains active. When a group is created, an expiration policy is associated with it, by default. This default expiration policy may vary depending on the expiry settings. For information about these settings, see **Expiry Settings** later in this section. You can change the expiration policy for groups any time. The Group Management Service is responsible for expiring groups when their period is over. You can set the service to notify the group owners or the default approver about the expiry. For more information about these settings, see **Expiry Settings** later in this section. The expiration process is automatic, however, you can also manually expire groups overlooking their expiration policy.

Expire groups using an expiration policy

To change the expiration policy of a group, follow the instructions below:

1. Expand the **Automate** node and select the required group node.
2. From the groups list, right-click the required group and then click **Properties**. This displays the **Properties** dialog box for the selected group.
3. Click the **General** tab, if not already selected.
4. In the **Expiration Policy Settings** area:
    i. From the **Expiration Policy** list, click the required expiration criteria. For example; if you want to expire the group after a year, click **Expire Every Year** in the list.
    ii. When the confirmation message shows, click **OK** to confirm the policy. You will notice that the **Expiration Date** on the Properties dialog box is updated according to the selected expiration policy.

The **Expiration Policy** list is not available for Dynasty children since they inherit the expiration policy of their parent and you cannot change it explicitly for any child.

5. Click **OK** to close the dialog box.

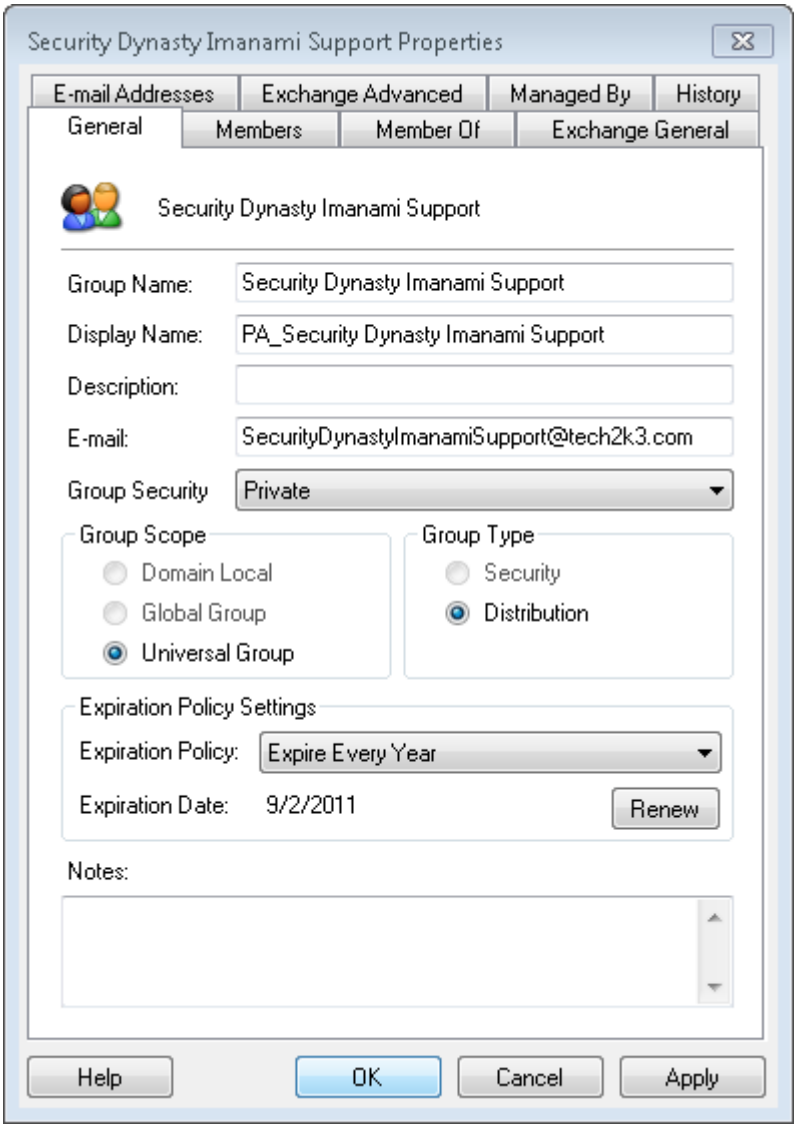


Figure - The General tab of the Properties dialog box

To change the expiration policy of multiple groups, follow the instructions below:

1. Expand the **Automate** node and select the required group node.
2. From the Groups list, select the required groups.
    - To select consecutive groups; click the first group in the list, press and hold down the **SHIFT** key and then click the last group.
    - To select non-consecutive groups, press and hold down the **CTRL** key and then click each group that you want to select.
3. Right-click the selected groups, point to **Set Expiration Policy to** and click the required expiration policy.
4. Click **Yes** on the confirmation dialog boxes to confirm the change.

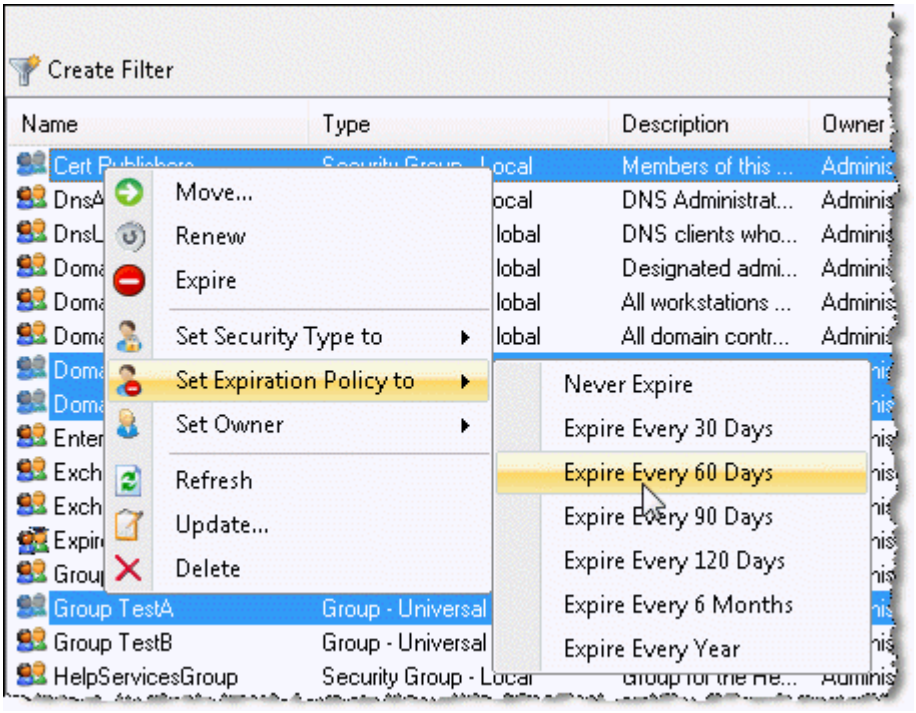


Figure - The Set Expiration Policy to command on the shortcut menu

Expiring groups manually

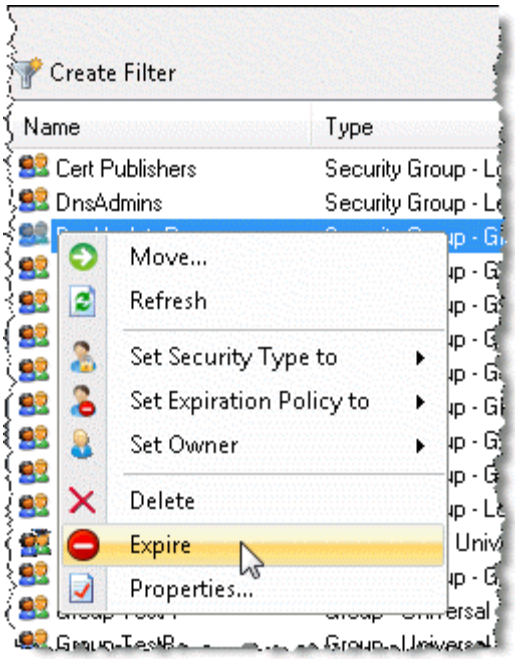


Figure - The Expire command on the shortcut menu

When a group expires, "EXPIRED_" prefix is added with the group name and it moves to the **Expired Groups** node.

Renewing Groups

If a group has expired and you still need the group, you can renew it. If a group is not renewed within the time frame that is specified in the system configuration settings of GroupID, it is automatically deleted from Active Directory. For information about automatic deletion of expired groups, see **Deletion Settings** later in this chapter.

To renew groups, use the following instructions:

1. Expand the **Automate** node, next expand the **All Groups** node and click **Expired Groups**.
2. From the groups list, select one or more groups as required:
    - To select consecutive groups; click the first group in the list, press and hold down the **SHIFT** key and then click the last group.
    - To select non-consecutive groups, press and hold down the **CTRL** key and then click each group that you want to select.
3. Right-click the selection and click **Renew**.

Dynasty children automatically renew with their parent. Renewing them explicitly is not allowed.

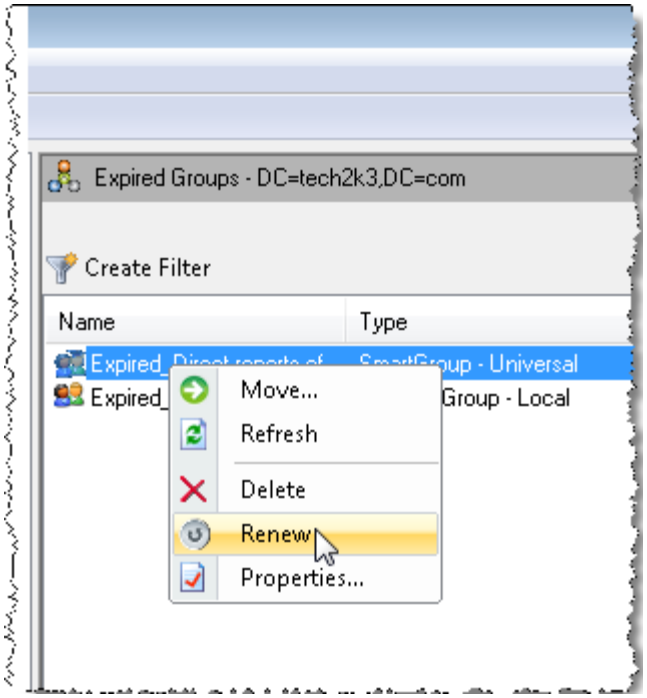


Figure - The Renew command on the shortcut menu

When you renew a group, its last expiration policy is applied to it.

Expiry Settings

Group expiry is a part of the GroupID GLM feature that lets you control the lifecycle of a group in your directory. Expiry settings control the default behavior of expiry policy for groups and the wait period for deleting a group after it expires. Some of the global settings can be overwritten for groups individually.

To configure expiry settings:

- In GroupID Management Console, click the **Configuration** node and then click **Modify System Configurations**. This displays the **Configurations** dialog box. On the **Configurations** dialog box, expand **Client** and then click **Group Lifecycle**.

The following sections cover the Group Lifecycle settings available on the Configurations dialog box.

Security group expiration

Security group expiration is a GLM feature that applies and enforces lifecycle management of security groups in particular. In the availability of this feature, the members of an expired security group will be granted or denied access to any network resources that have been assigned to it. This is in addition to the other actions that are carried out on expired groups by GroupID.

A security group may grant or restrict its members access to network resources. If a security group is set to restrict access to certain resources then it should be the part of an organizational unit on which the expiration policy does not apply. Such OUs can be specified by adding them to the Excluded OUs list on the **Group Lifecycle** tab of the **Configurations** dialog box. This is recommended because if this security group expires, the members of this group will gain access to all the restricted resources.

To enable security group expiration:

- In the **Security Group Expiry Settings** area, select the **Enable Security Group Expiration** check box.
- Click **OK**.

Selecting the default expiration policy

This will set the default expiration policy for the new groups that users create in Automate. Setting a default expiration policy only controls the default selection to set when a new group is created and does not restrict the user from changing it.

- In **Group Lifecycle** settings, use the **Default Expiration Policy** list to select the required policy to set as default.
- Click **OK**.

Filter groups for expiration

By default, the Group Management Service processes groups of all organizational units for automatic expiry and deletion. You can filter organizational units that you want to include in or exclude from the GLM feature.

1. In **Group Lifecycle** settings, click one of the following options:
    - **Include OUs**, if you want to select organizational units that you want to participate in the group lifecycle. The Group Management Service will only process groups in the selected organizational units and ignores the rest.
    - **Exclude OUs**, if you want to select organizational units that you want to exclude from the group lifecycle. The Group Management Service will process groups of all organizational units except the selected ones.
2. Use **Modify** below the **Exclude/Include groups in the following OU's from/into expiration** list to select organizational units you want to include or exclude according to the option selected above.

3. Click **OK**.

Notifications for expiring groups

Expiring groups can generate notifications sent to the owners or the default approver (if a group has no owner) to inform them about their approaching expiry date. Based on the requirement, the owner may change the expiry policy of their group to extend its expiry period or they may ignore the notices to let the group expire and be removed from the directory. Use the following to set notifications in GroupID.

- From the **Notify owner of group expiration** list, select one or more of the following options:
    - **1 day before expiration**, to send the expiry notification e-mail to group owner a day before the group expires.
    - **7 days before expiration**, to send the expiry notification e-mail to group owner 7 days before the group expires.
    - **30 days before expiration**, to send the expiry notification e-mail to group owner 30 days before group expiry.
- Click **OK**.

Group owner notification settings require notifications to be enabled which can be configured using the **Notification** settings on the **Configurations** dialog box.

If no option is selected for expiry notifications, no notifications will be delivered even if the group has owners or a default approver is set.

Set default approver for notifications

If expiry notifications are enabled, the Group Management Service requires a person to whom the notifications will be sent for the expiry. By default, the group owners are designated as the notifications receivers. For the groups without owners (primary or additional), you can designate a user to whom the expiry notifications will be sent. If no default approver is set, the Group Management Service will not expire the groups without owners.

- Click **Browse** next to the **Default Group Approver** box. This displays the **Default Group Approver** dialog box.
    - On the dialog box, type the name of the user that you would like to set as the default notifications approver and click **Check Names**.
      If your entered name results in multiple matches, a **Matching Objects** dialog box will be displayed for you to select the required object.
- Click **OK**.

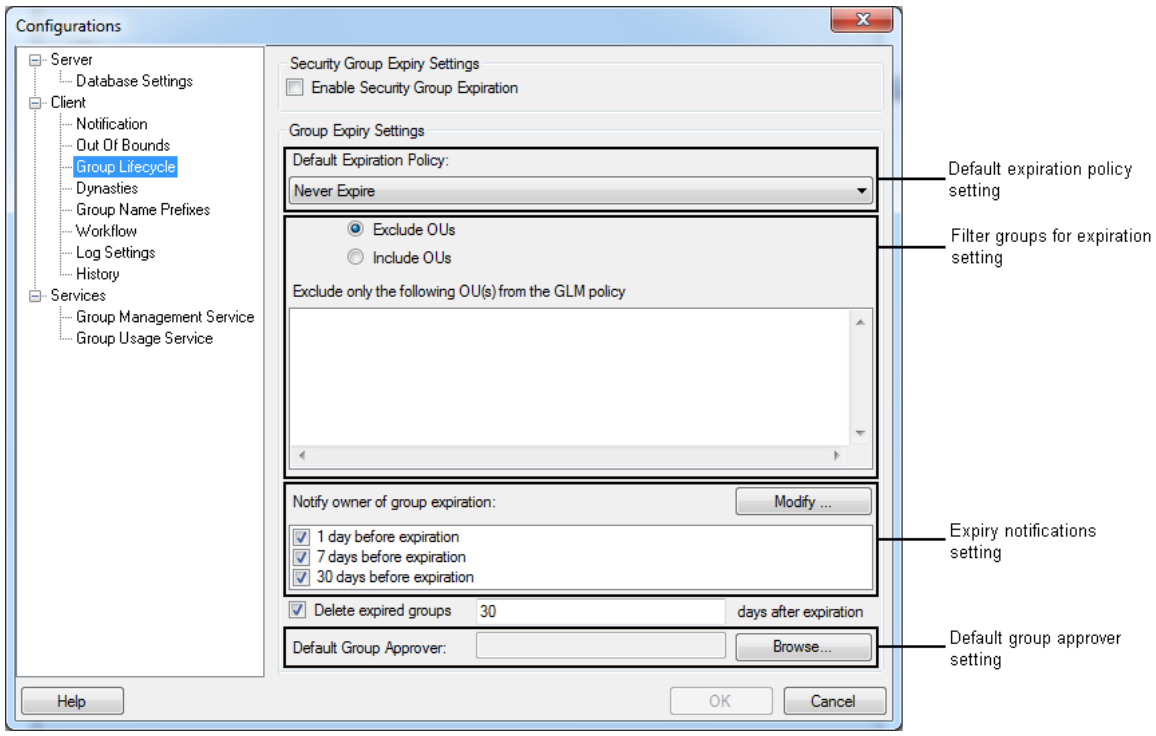


Figure - Group lifecycle expiry settings on the Configurations dialog box

Deleting Groups

Groups in Automate can either be deleted interactively or automatically. The concept of both deletion methods is covered in the topic **Group** of **Chapter 2: Group Management Concepts**. The interactive method results in physically deleting groups where the deleted groups are moved to the **Recycle Bin** from where they can be restored if required. The automatic method results in a logical deletion and this action is carried out by the Group Management Service that automatically deletes an expired group after particular period of its expiry and notifies the owners or the default approver (in case no owner is set for the group) about the deletion. If a group has no owner and no default approver is set in the global settings too, the service will not delete the group. The deletion period is set to 30 days by default. However, this setting is configurable using the global settings. For information about changing the deletion period, see **Deletion Settings**. If a logically deleted group is still needed, you can simply renew it. Both logically and physically deleted groups are locked for any further operations.

Deleting groups physically

1. Expand the **Automate** node; select the required group node.
2. From the groups list, select one or multiple groups as required:
    - To select consecutive groups; click the first group in the list, press and hold down the **SHIFT** key and then click the last group.
    - To select non-consecutive groups, press and hold down the **CTRL** key and then click each group that you want to select.

    Right-click the selection and then click **Delete**.

This displays a confirmation message. Click **Yes** on the message to delete the groups.

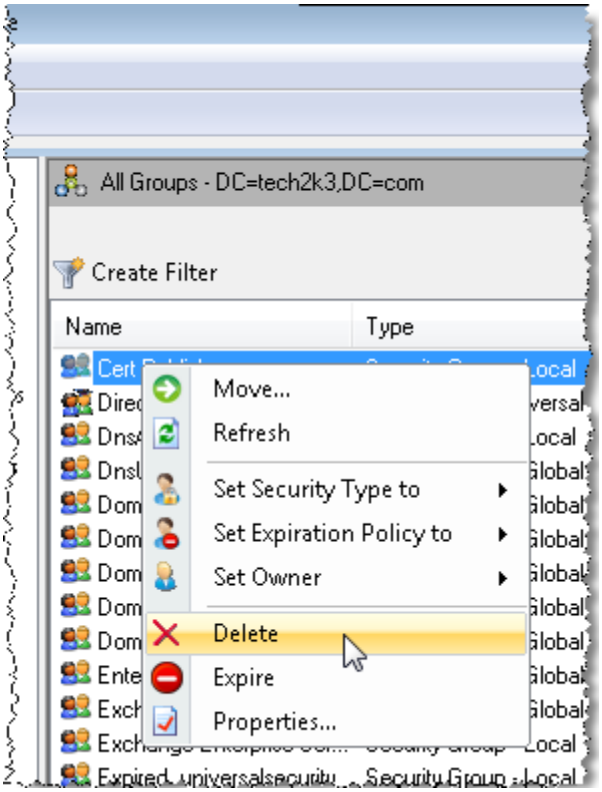


Figure - The Delete command on the shortcut menu

Deletion Settings

You can set the days after which the expired groups should be automatically deleted.

Requires Self-Service license

The instructions below list the procedure for this:

- On GroupID Management Console, click the **Configuration** node and then click **Modify System Configurations**. This displays the **Configurations** dialog box. On the dialog box:

  i. Expand **Client**, and then click **Group Lifecycle**.

  ii. Select the **Delete expired groups** check box, then type the number of days in the given box after which you want to automatically delete the expired groups.

  iii. Click **OK**.

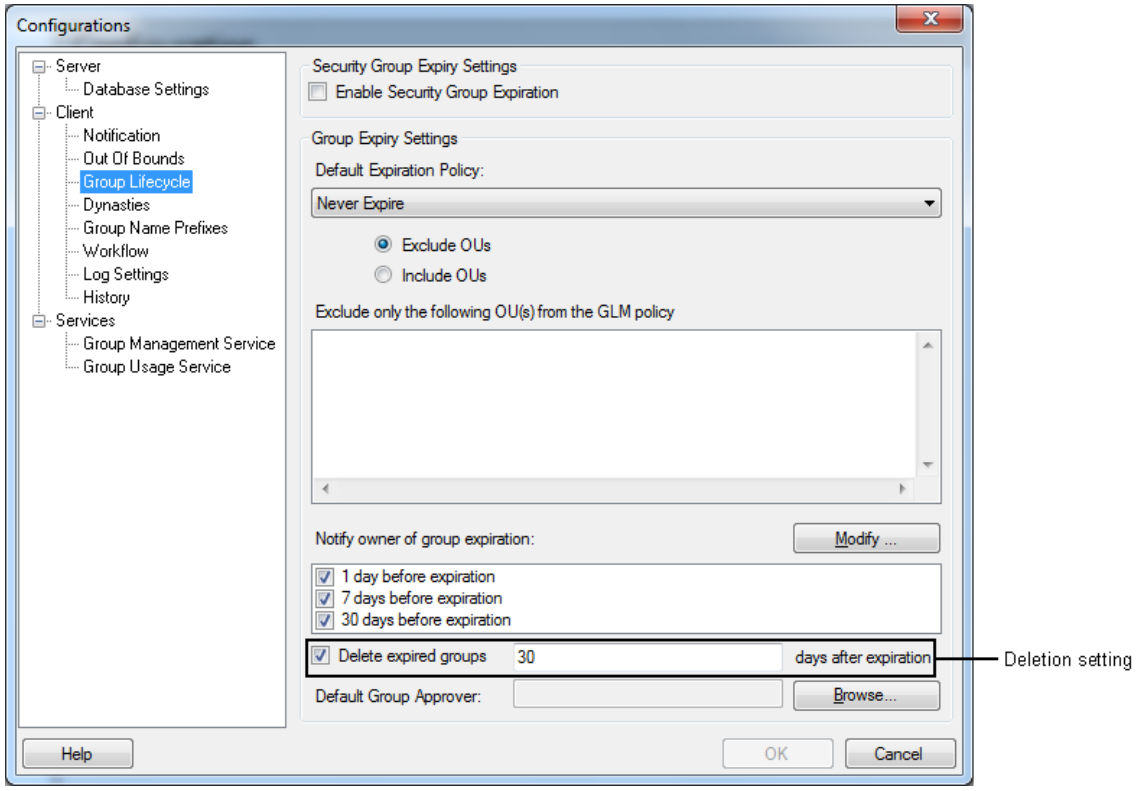


Figure - Highlights the deletion setting related to the expired groups

Recycle Bin

When a group is physically deleted (using the shortcut menu or the Actions menu), it is moved to Recycle Bin. The concept of physically deleted groups is covered in the topic **Group Deletion** of **Chapter 2: Group Management Concepts**. If you have deleted the group mistakenly and it is still needed, you can simply restore it from there.

To restore a group from Recycle Bin:

1. Expand the **Automate** node and click **Recycle Bin**.
2. From the groups list, locate the group you want to restore.
3. Right-click the group and click **Restore** on the shortcut menu.
4. Click **OK** on the confirmation dialog box.

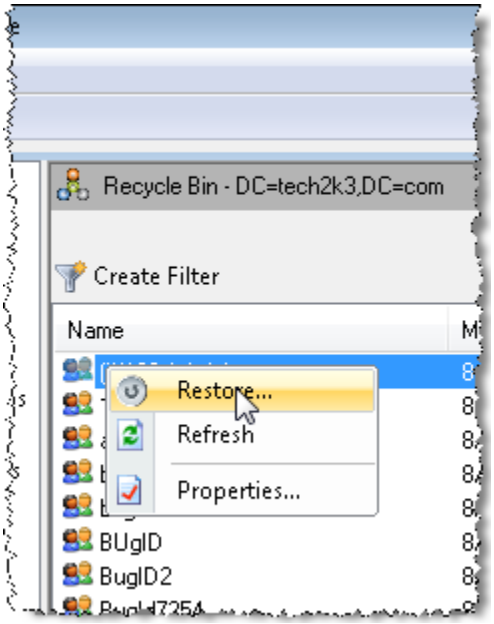


Figure - The Restore command on the shortcut menu

Group History

GroupID maintains a complete track of actions performed on a group since its creation. The actions that GroupID tracks depend on the history settings configured on the Configuration dialog box. The list of actions GroupID can have a track of are explained in detailed in the topic **History Settings** in **Part 7: GroupID Configurations**.

GroupID offers two views of history records for a group:

- Normal View
- Detailed View

Normal View

The normal history view is what you see on the **History** tab of a group Properties dialog box. A normal history view of a group comprises of the following items:

- **Time**, at what date and time, the action was performed.
- **Action**, the type of action performed.
- **Attribute**, what Active Directory attribute is changed due to the action.
- **New Value**, the changed value.
- **Old Value**, the old value before the change was applied.

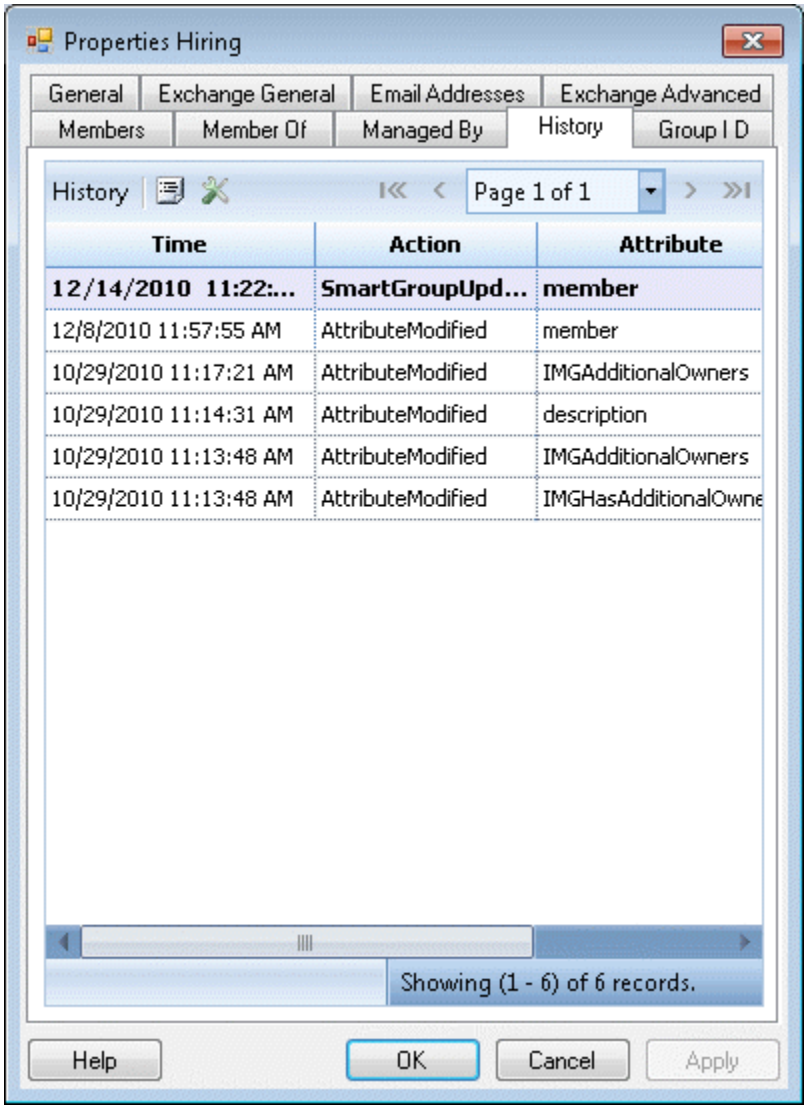


Figure - The History tab showing the normal history view

Detailed View

The detailed history view is shown when you select a history record in the normal history view on the **History** tab and click the **View Details** icon. A detailed history view of a group comprises of the following items:

- **Who**, the name of the person who performed the action.
- **What**, the action performed.
- **When**, the date and time of action.
- **Module**, the name of the module using which the action was performed.
- **Where**, the machine name from where the action was performed.

If the target attribute is single-valued, the following items will be shown:

- **Old Values**, the list of values before the action was performed.
- **New Values**, the list of values after the action was performed.

For multi-valued attribute, the following items will be shown:

- **Added Items**, the list of items that were added to the multi-value attribute.
- **Removed Items**, the list of items that were removed from the multi-value attribute.

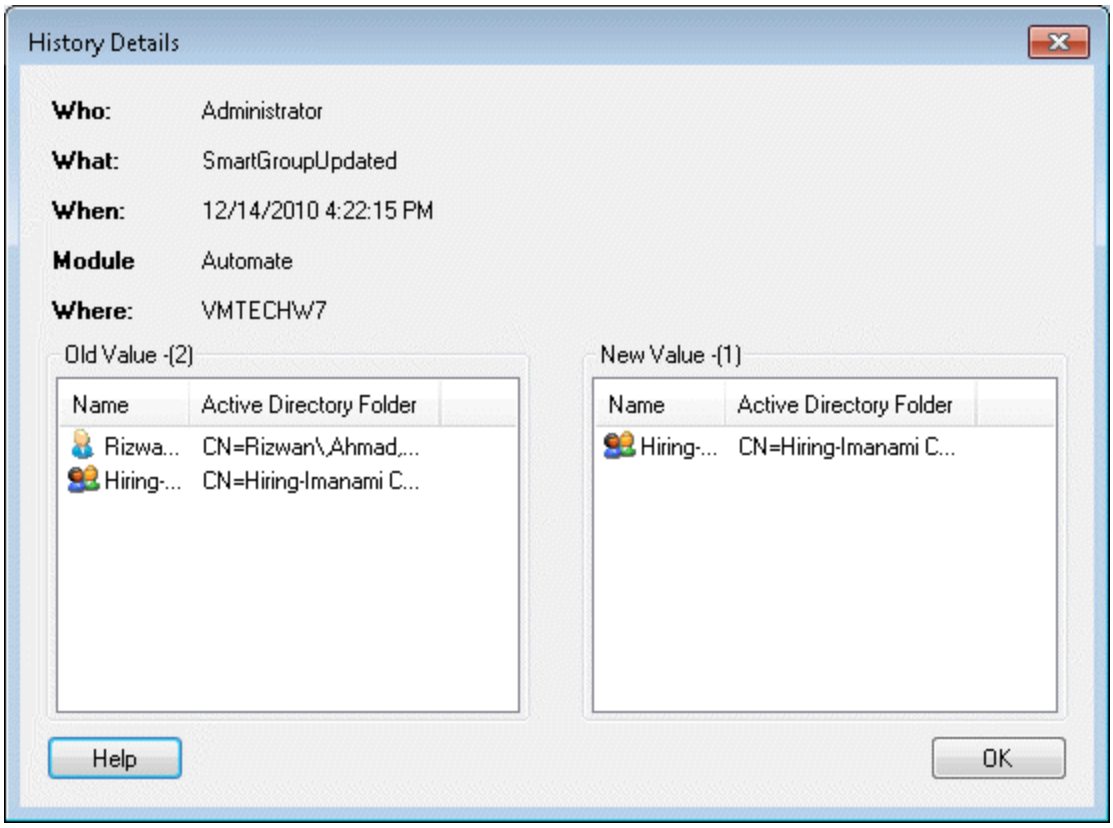


Figure - The Detailed View of a History record of single-valued attribute

Group Management Service

Group Management Service is responsible for expiring or logically deleting a group and sending notifications for these actions. For detailed information about logically deleted groups, see **Group Deletion** in **Chapter 2: Group Management Concepts**. These notifications contain URLs that redirect them to Self-Service Portal pages where they can take the necessary actions accordingly. The service runs in the background and watches the lifecycle policies of all groups. When a group is about to expire, the service automatically sends the expiry notification to its owners and when the expiry period is over, it deletes the group.

The service is installed with Self-Service and is available in the Windows Service Manager by the name Imanami Group Management Service. From GroupID Management Console, this service can be controlled using the **Group Management Service** settings on the **Configurations** dialog box. One instance of the Group Management Service will maintain management of multiple domains in the same forest.

Adding domains

Use the instructions below to add domains that you want the service to process:

1. On GroupID Management Console, click **Configuration**, and then click **Modify System Configuration**.

2. On the **Configurations** dialog box, expand **Services**, and then click **Group Management Service**.
   This shows the **Entire Directory** node expanding which shows all domains and sub-domains within the forest where your logged on domain exists.

3. Select one or more domains for which you want the Group Management Service to expire or delete groups by following any of the options below:

   i. **To select all domains**, click in the check box available with **Entire Directory**. This displays the **Configuring Default GLM Service** dialog box, where:

      a. In the **User Name** box, type the user name of account with which to connect.

      b. In the **Domain** box, type the domain in which the specified user name exists.

      c. In the **Password** box, type the password for the specified user.

      d. From the **Self-Service Portal URL** list, select a Portal's URL. This URL sets the Self-Service Portal to redirect the users for taking an action against notifications. The URL for the selected Portal will be included in the e-mail notifications generated for group activities (expiry, deletion, membership changes). If no Portal is created yet, click the **Create a Self-Service Portal...** option in the list to create the Portal. For information about creating a new Portal, see **Create a new Portal** in **Chapter 4: Setting Up a New Portal**.

      e. Click **OK** to close the dialog box.

   The configurations provided for Entire Directory will be applied to all domains in the forest which can be changed individually by right-clicking the domain and clicking **Properties**.

   ii. **To select individual domains,** select the check box available with the domain name to display the **Configuring [*domain name*]** dialog box and then follow the steps 3(i)(a) to 3(i)(e) for adding credentials.

4. Click **OK** to save the domain settings.

Individual domain configurations take precedence over the configurations provided for the entire directory.

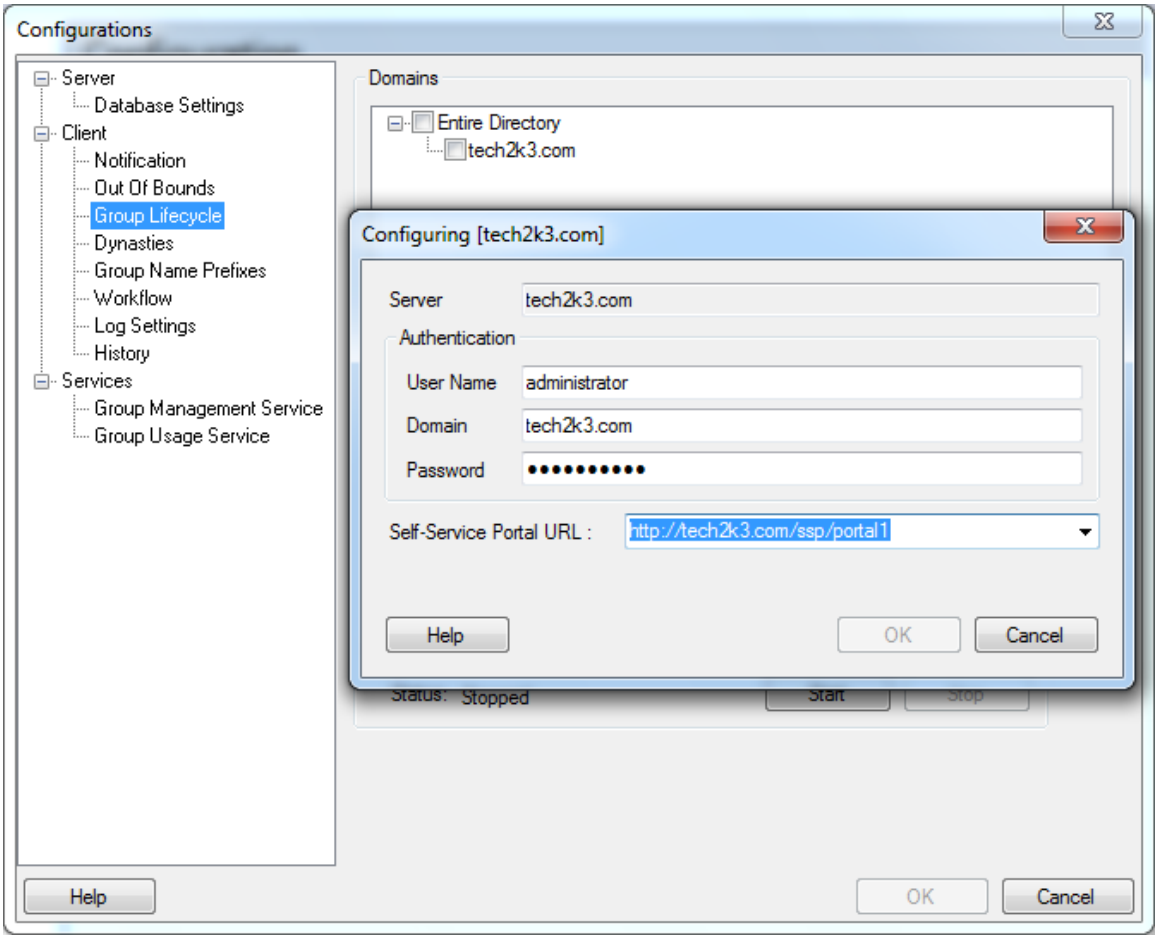


Figure - Group Management Service settings

Starting the Group Management Service

By default, Group Management Service is stopped when you install GroupID. To start the service, click the **Start** button in the **Service Status** area. It is not necessary to stop the service for adding new domains.

Chapter 10: Memberships

This chapter explains fundamental concepts that you must know about group memberships and provides instructions on how you can manage them.

Group, explains different ways of adding members to a group.

Nesting, provides an overview of nesting groups and instructs you on how you can implement nesting.

Membership, covers the information about configuring different membership settings.

Group Members

Groups are created to apply a common set of policies on multiple objects. This helps in saving time by simply adding new members to a particular group depending on the privileges and permissions they require instead of setting them individually for every member.

Members can be added to a group a couple of different ways. These are:

1. **Manual**

   You can manually add members to a group any time when required. This can be for both managed (SmartGroups) and unmanaged groups. For more information about adding members manually, see **Adding Memberships** later in this chapter.

2. **Automatic**

   The memberships of SmartGroups can automatically be updated using user-defined queries in combination with job schedules. For more information about automatic update, see **Updating Groups** in **Chapter 9: Managing Groups**.

3. **Using Import Group Membership wizard**

   In this method, you specify an external data source containing the data for the objects to add as members to the selected group. The data from the external data source is matched with the objects in your Active Directory based on the field mapping defined in the query designer. For records where the values for the mapped fields match, the wizard adds the object as a member to the selected group. For more information about importing membership from external data source, see **Importing** later in this chapter.

Adding Membership

1. On GroupID Management Console, expand the **Automate** node and click the required group node for the group you want to add members.
2. Right-click the required group and then click **Properties**. This displays the Properties dialog box for the group.
3. On the dialog box, click the **Members** tab and then click **Add**. This displays the **Find** dialog box, where you can search for the Active Directory objects, such as users, contacts and similar that you want to include in the group.
4. Click **OK** when done to close the dialog box and add the selected objects to the group.
5. Click **Apply** and then click **OK** to save changes.

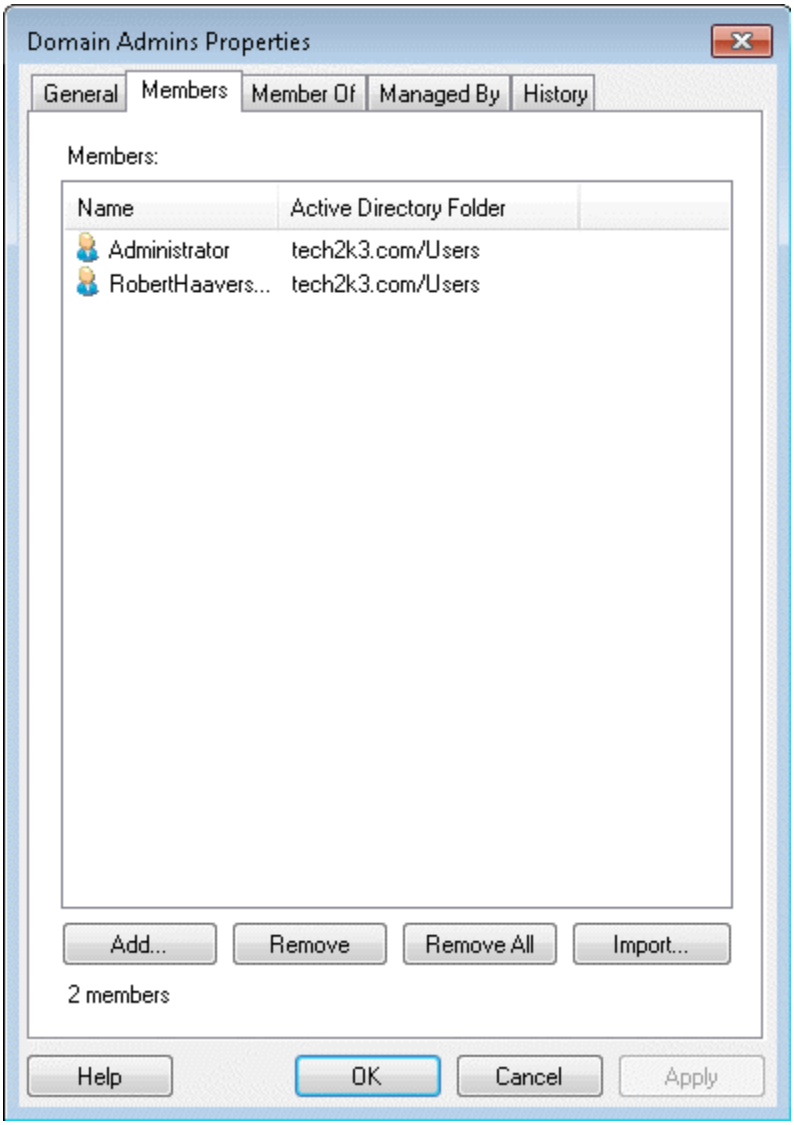


Figure - The Members tab

Removing Membership

1. Select the required group for which you want to remove members.
2. Right-click and then click **Properties**.
   This displays the Properties dialog box for the group.
3. On the dialog box, click the **Members** tab.
4. From the **Members** list, select the member to remove and click **Remove**. To select multiple members, press and hold the **CTRL** key while clicking the members in the list to remove. Use **Remove All** to remove all members of the group given in the list.

Importing Memberships

The Import Group Membership wizard lets you specify an external data source from which it matches the list of members to import from Active Directory into the group. For example, you have a list of Employee-IDs in a text file and you want to add all employees from Active Directory, whose IDs match with those present in the text file, to the membership of the group. All you need to do is to select the text file and map its field name with the **employeeID** attribute of the directory. The wizard will search the directory for all objects having employeeIDs same as mentioned in the text file and add those in the membership of the group.

The instructions below guide you on how you can use the Import Group Membership wizard to import members to a group:

1. Expand the **Automate** node and click the required group node for the group of which you want to import members.

2. Right-click the required group, and then click **Properties**. This displays the **Properties** dialog box for the group.

3. On the dialog box, click the **Members** tab and click **Import**. This launches the **Import Group Membership** wizard.

4. On the first page of the wizard, read the welcome message and click **Next**.

Import Group Membership
Introduction
Data Provider
Import Options
Completion
Welcome to the Import Group Membership wizard.
This wizard allows you to import your group membership from a source other than Active Directory. This is helpful when you have, for example, a text file from another system that contains the recipients that you want to be a member of this group. As long as the text file contains data that can be resolved in your Exchange or Active Directory, GroupID can update the membership of the group.
Help
Next >
Cancel

Figure - The Welcome page

5. On the next page of the wizard, select and configure the data source with which you want to connect for obtaining the list of values whose matches you want to import from Active Directory.

6. Click **Next**.

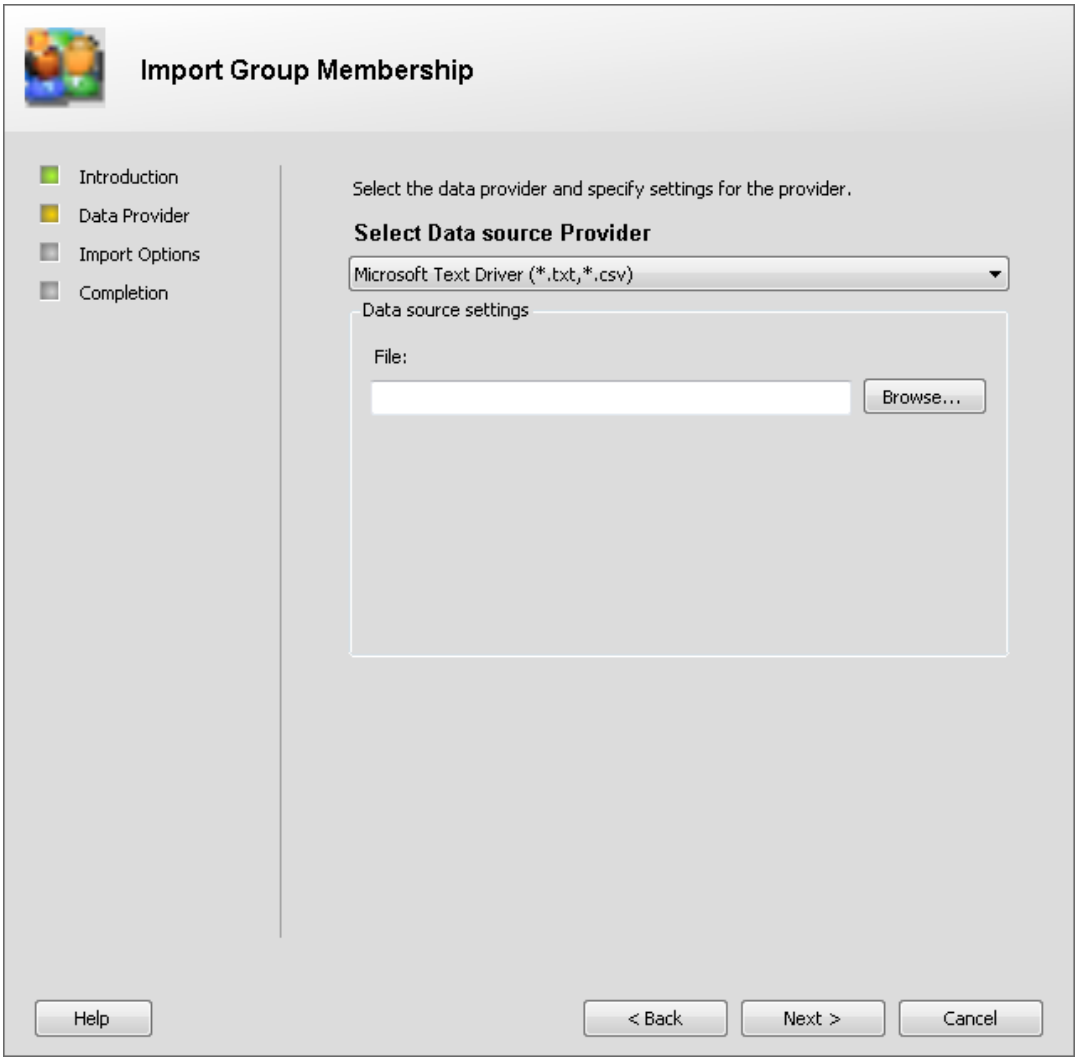


Figure - The page where you select the source data provider

7. On the **Import Options** page, select the source container and map the fields for the data source and Active Directory. On the basis of this field mapping, the wizard will determine the memberships to import by matching the values of the two fields.

    i. Click **Browse**, to open the **Select Container** dialog box and select the top level Active Directory container to look in for the member objects.

    ii. From the **Source field** list, select the name of the field, from the source, to map with its related Active Directory field.

    iii. From the **Directory field** list, select the name of the Active Directory field to map with the selected source field. The wizard will import memberships where values for both the fields will match.

    iv. You can click **Preview** to view the values returned as a result of the selected fields.

8. Click **Next** to start the import process.

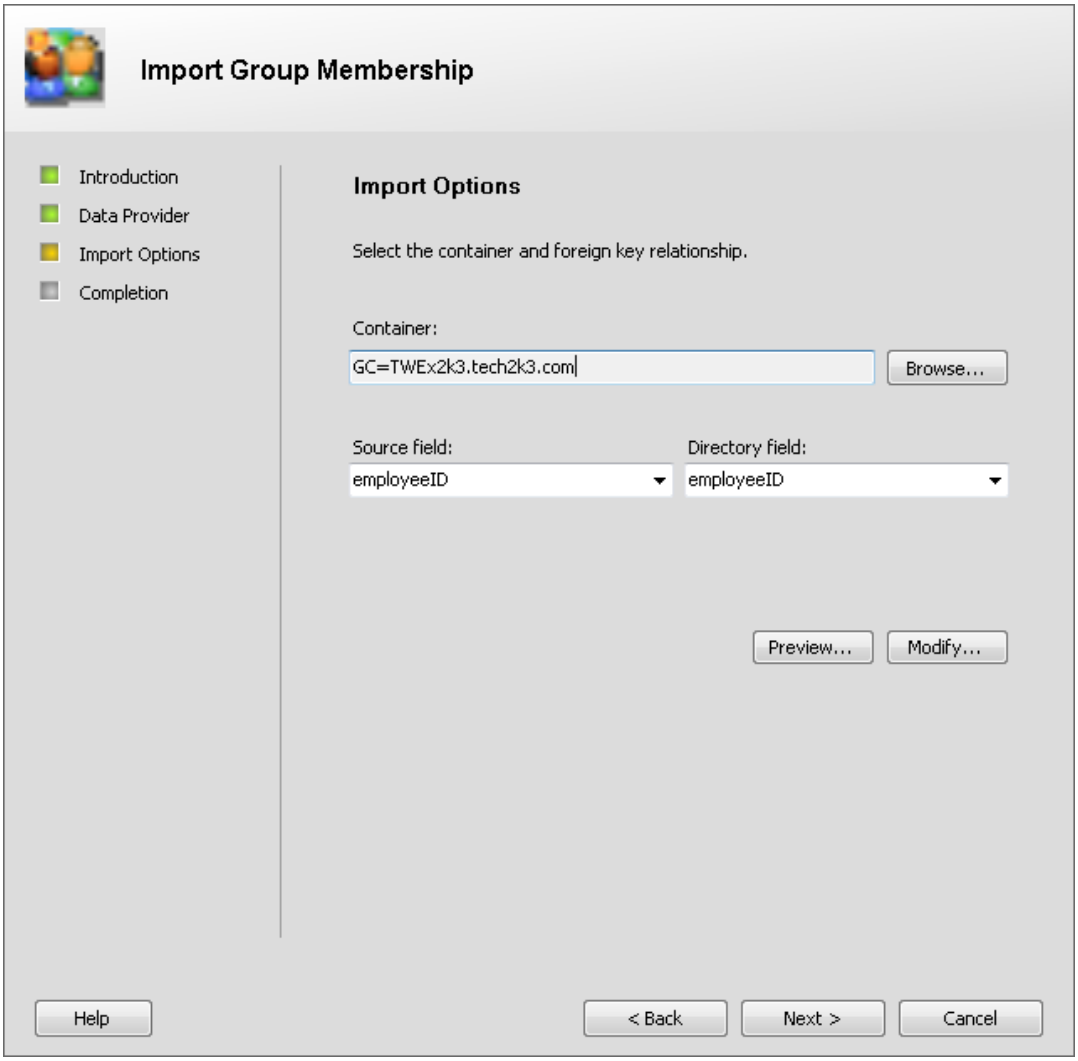


Figure - The Import Options page

9. Once the process completes, click **Finish** to close the wizard.

Nesting Groups

Adding a group as a member of another group is called **nesting**. You nest groups to consolidate member accounts and reduce replication traffic. Nesting option depends on the domain functionality mode (native or mixed) of your Windows server and the group type. For distribution groups, nesting is supported in both mixed mode and native mode. For security groups, nesting is supported only for domains running in native mode. Before nesting groups, be aware that depending on the scope of the group, the group can contain only specific types and scopes of other groups.

The following list describes what a group in native-mode domain can contain. The same applies to distribution groups in mixed-mode domains:

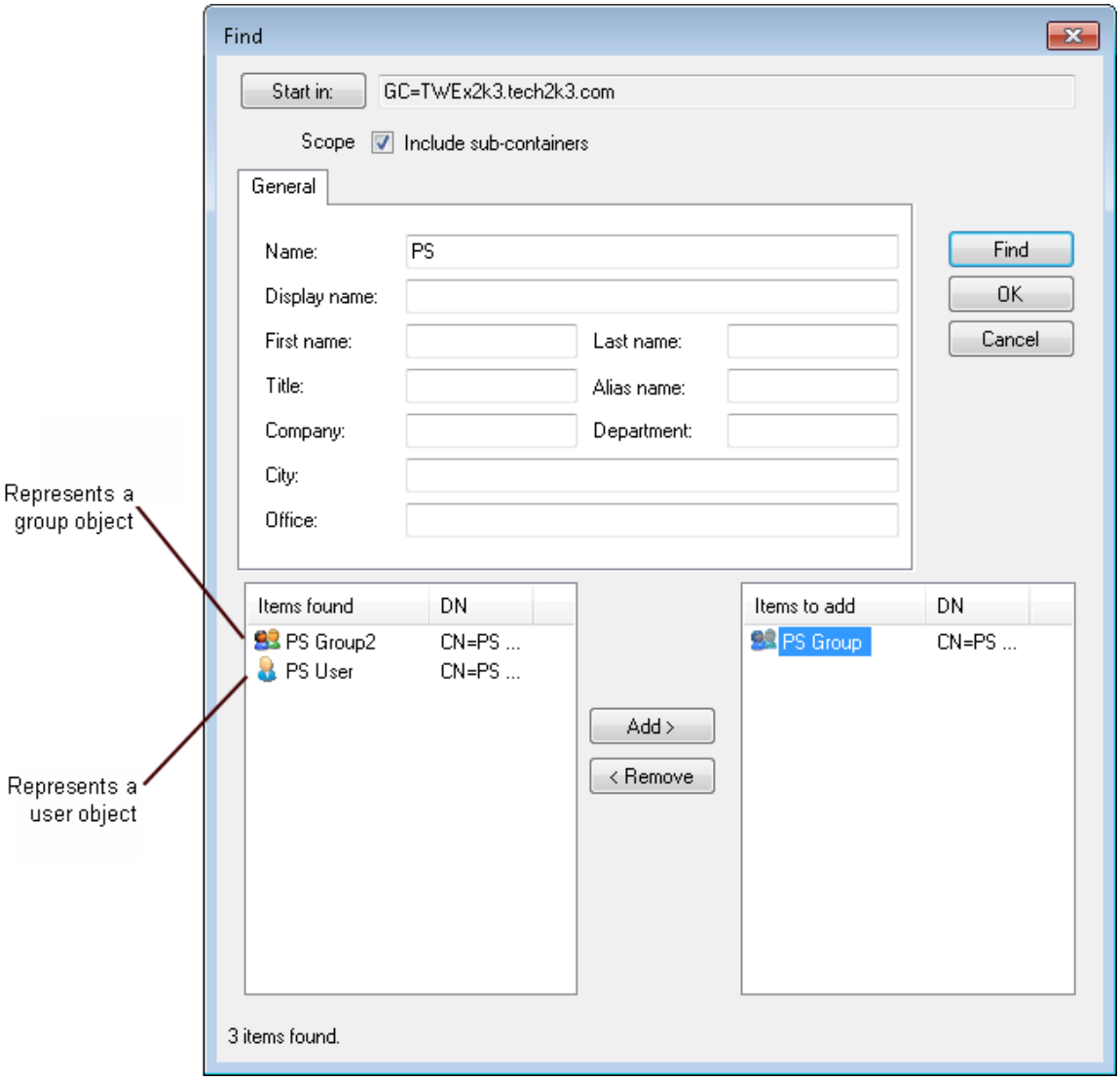
- A universal group can contain other universal groups, global groups and accounts from any domain in any forest. A universal group cannot contain any domain local groups.
- A global group can contain other global groups and accounts from the same domain that the group belongs to. A global group cannot contain any universal groups, or any global group or account from another domain.
- A domain local group can contain universal groups, global groups and accounts from any domain or forest. A domain local group can also contain other domain local groups from the same domain that the group belongs to. A domain local group cannot contain other domain local groups from any other domain or forest.

Security groups in a mixed-mode domain have the following restrictions:

- Universal groups cannot be created in mixed-mode domains because the universal scope is supported only in Windows 2000 native-mode domains.
- A global group can contain accounts from the same domain to which the group belongs. A global group cannot contain any universal groups, any global group, or an account from another domain.
- A domain local group can contain global groups and accounts from any domain or forest. A domain local group cannot contain any other domain local group.

Making a Group Member of Other Groups

The steps for adding a group as the member of another group are same as provided for **Adding Membership** earlier in this chapter. On the **Find** dialog box, you need to search and select a group object from the Items found list.



Removing a Group's Membership

For removing a group from the membership of another group, use the same steps as mentioned in **Removing Membership** earlier in this chapter.

Membership Settings

You can configure membership settings that are applicable to all SmartGroups. These setting are explained in the following sections:

- Setting the Maximum Members Limit for the Group
- Setting Maximum Members Threshold Limit

Setting the Maximum Members Limit for the Group

You can specify a limit of maximum members that can be added to a SmartGroup when its membership is updated based on a user-defined query. If the query's result set exceeds the specified limit, the default settings of Automate will not add members to the group retrieved by the query. However, you can change this setting to break the group into smaller groups and divide members into these groups when the maximum member per group is reached. In this scenario, all sub-groups that are created as a result of the division are added to the membership of the parent group.

Use the instructions below to set the maximum limit:

- In the tree view of GroupID Management Console, click **Configuration** and then click **Modify System Configurations**. This displays the **Configurations** dialog box. On the dialog box:

    i. Expand **Client**, and then click **Out of Bounds**.

    ii. In the **Maximum members per group** box, type the number that you want to set as the maximum limit for group members.

    iii. Click **OK**.

Divide members into child groups

If you want to divide a group into child groups when the membership exceeds the above specified limit, click **Nest into child groups** in the **Maximum membership** area.

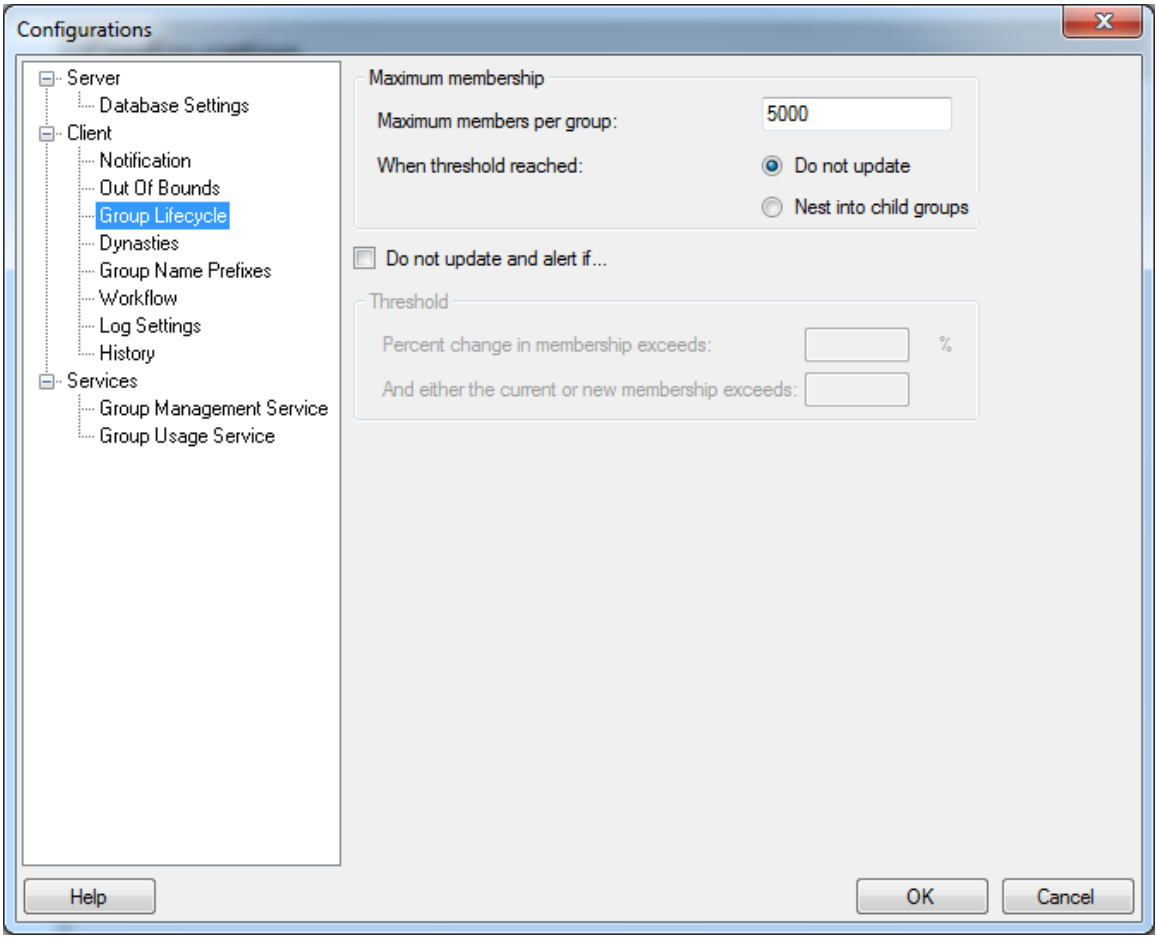


Figure - The Out of Bounds settings

Setting the Maximum Members Threshold Limit

You can set Automate to handle out-of-bound exceptions. These exceptions are designed to prevent large disastrous changes from happening to group membership. When an out-of-bounds exception occurs, the group membership is not updated and the owner or administrator is notified by e-mail (requires Notifications to be enabled which can be configured using the **Notification** settings on the **Configurations** dialog box). If the owner/administrator determines that the change is valid, they can update the group manually.

Use the instructions below to set the maximum members threshold limit:

- On GroupID Management Console, click **Configuration** and then click **Modify System Configurations**. This displays the **Configurations** dialog box. On the dialog box:

    i. Expand **Client**, and then click **Out of Bounds**.

    ii. Select the **Do not update and alert if** check box. This makes the **Threshold** area available, where:

a. In the **Percent change in membership exceeds** box, enter a number indicating the membership change threshold (in percentage). If a change in membership exceeds this threshold it will trigger the out-of-bound exception. The percentage is calculated as: (Number of new members - Number of old members) / Number of new members.

b. In the **And either the current membership or new membership exceeds** box, type the maximum number of current membership or new membership exceeding which will cause the out-of-bound exception to occur.

Out-of-bound exception will occur if both the **Percent change in membership exceeds** and the **And either the current membership or new membership exceeds** conditions are met.

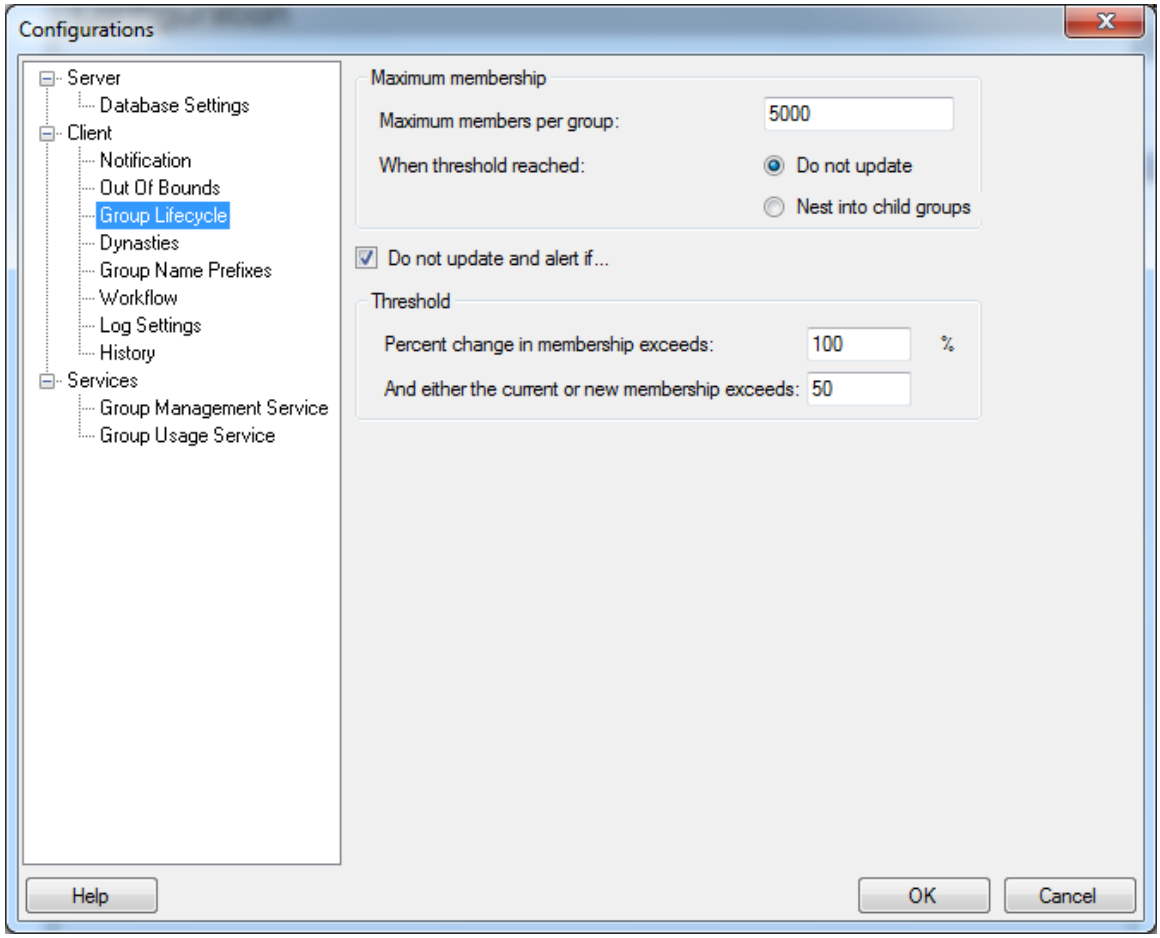


Figure - The Threshold settings. The Threshold area becomes available on selecting the Do not update and alert if check box.

Chapter 11: Exchange Settings

This chapter covers all Exchange settings which are available to you if you are connected to an Active Directory domain controller with Microsoft Exchange Server deployed in the forest. The chapter is divided into following sections:

- Exchange, introduces you with the exchange related tabs on the Properties dialog box.
- Applying Size Limit to Incoming Messages, explains how you can apply size limit to all incoming messages to a particular group.
- Restrict Recipients for the Group, explains how you can restrict the group to accept messages from a particular recipients list.
- Selecting Expansion Server, provides instructions on selecting the Expansion server.
- Hiding Group, describes how you can prevent a group from appearing in Exchange address lists.
- Hide Group, explains the process of hiding group members from the Outlook address book.
- Set Group, explains how you can configure out-of-office auto-replies.
- Set Recipient, instructs you about setting the recipient to whom the delivery failure report will be sent when a message is not delivered.
- Assign Values to Custom Attributes of a Group, explains how you can utilize custom attribute fields to save additional information about the group.

Exchange Settings tabs

If your GroupID Management Console is connected to an Active Directory domain controller with Microsoft Exchange Server deployed in the forest, you will see three additional tabs on the Properties dialog box of the group. These tabs are: **E-mail Addresses**, **Exchange General** and **Exchange Advanced**. This is how you determine whether the group is mail-enabled after creation.

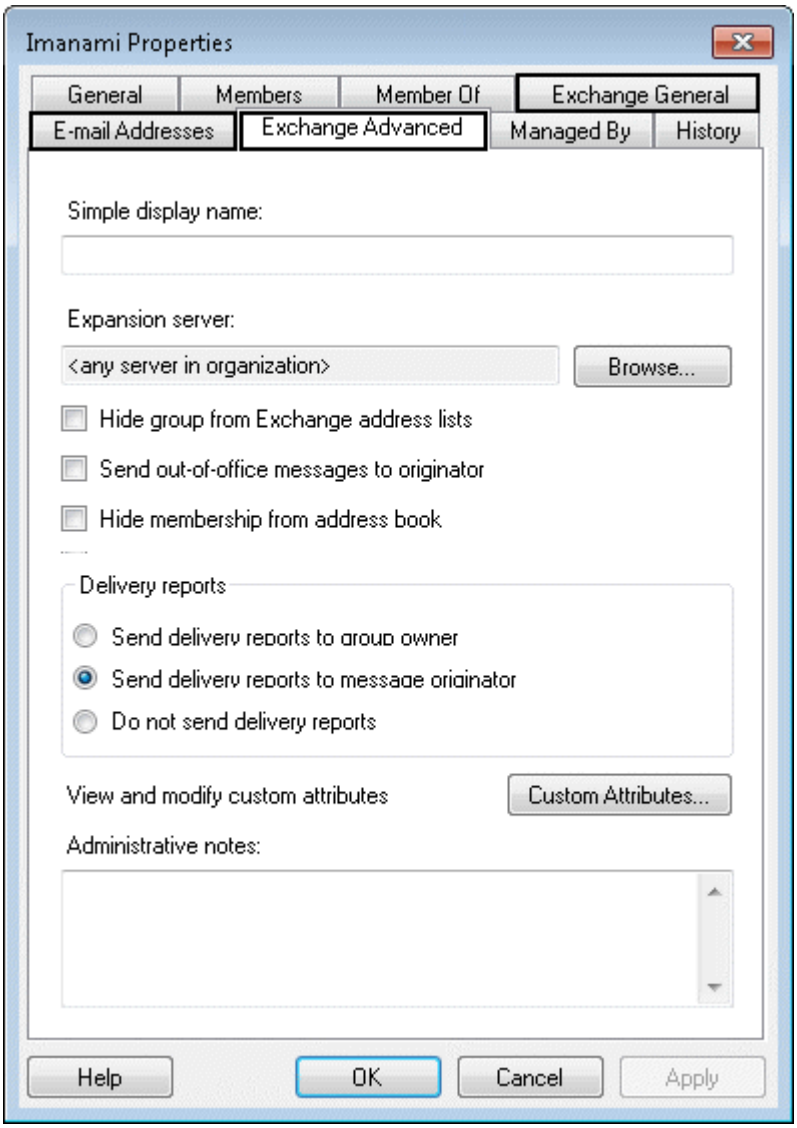


Figure - The Properties dialog box highlighting the Exchange tabs

The functionality of these tabs is explained below:

	Tab Name	Description
1.	E-mail Addresses	Lists all e-mail addresses assigned to the group. These addresses can be of different type; for example: SMTP, X400 and so on. You cannot add or remove e-mail addresses in the

	Tab Name	Description
		list.
2.	Exchange General	Lets you set general Exchange settings. You can change the display name, limit the maximum size of messages sent to the group, restrict the group from receiving messages from certain recipients and so on.
3.	Exchange Advanced	Allows you to configure advance Exchange settings. You can set the expansion server, prevent the group appearance on Exchange address list and Outlook address book, set recipients for non-delivery reports, customize the extension attributes and so on.

Applying Size Limit to Incoming Messages

The default Exchange settings apply no restriction on the incoming messages of the mail-enabled group. You can limit this size for a group, if required.

Use the instructions below to limit the message size:

1. On the Properties dialog box of the group, click the **Exchange General** tab.
2. In the **Message size** area, click **Maximum (KB)** and type the maximum message size (in kilo-bytes) the group can receive.
3. Click **Apply**.

Restrict Recipients for the Group

By default, all mailbox-enabled groups can accept messages from everyone in an Exchange organization. You can apply restrictions so that the group can accept messages from a specific list of recipients; or you can allow group to accept messages from everyone except a specific list of recipients.

Message restrictions can be applied to a mailbox-enabled group using the **Exchange General** tab of the Properties dialog box.

Allow group to receive messages from everyone

- In the **Message Restrictions** area, click **From everyone**.
- Click **OK**.

Allow group to receive messages from a specific list of recipients

1. In the **Message Restrictions** area, click **Only from**.
2. The **Apply a security quick filter** list provides you shortcuts for selecting recipients that the group can accept messages from. The options available in the list are:
    - **None**, select this option to allow everyone to send message to this group.

- **Owner + Members (good)**, select this option to allow only the members of the group itself and the owner, as specified on the Managed By tab, to send message to this group.

- **Owner only (best)**, select this option to allow only the owner, as specified on the Managed By tab, to send message to this group.

As you select an option from the **Apply a security quick filter** list, the recipients are shown in the bottom list accordingly which, for the **Only from** option, indicates the allowed recipient for the group. You can add more recipients in the list by clicking **Add** next to the list.

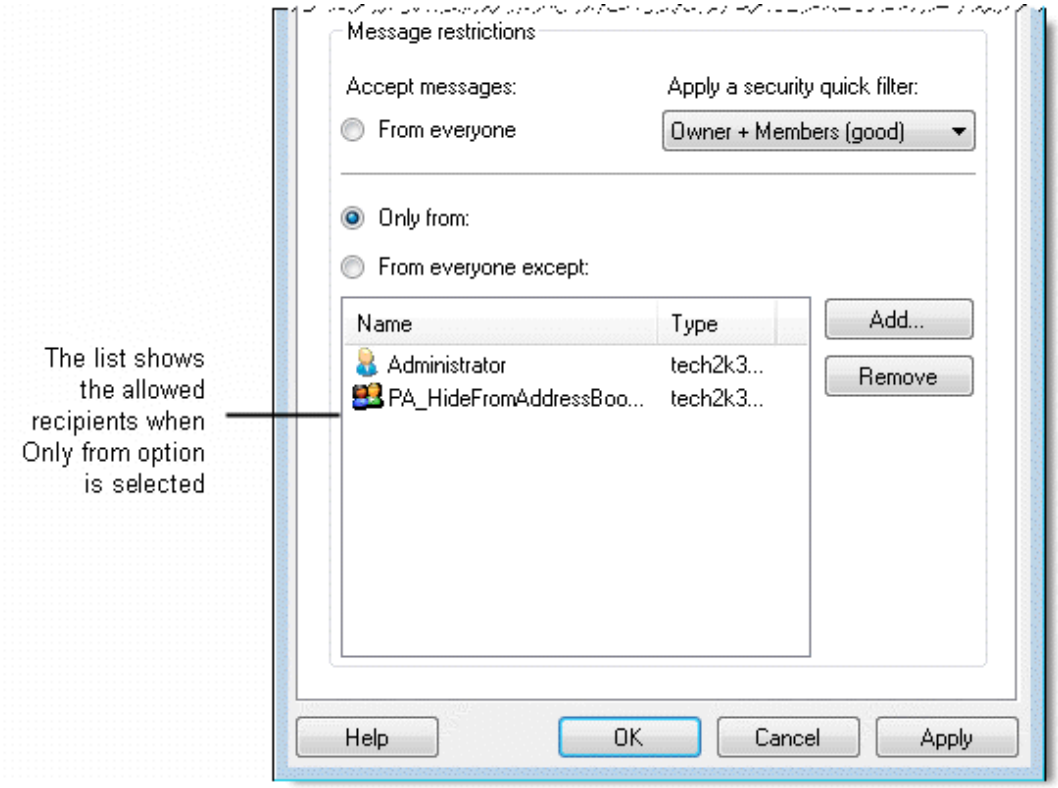


Figure - The list showing the allowed recipients

3. Click **OK**.

Restrict group to receive messages from a specific list of recipients

1. In the **Message Restrictions** area, click **From everyone except**.

2. Click **Add** next to the list available below **From everyone except**. This displays the **Find** dialog box where you can search and select the required recipients. As you select recipients on the Find dialog box, they are shown in the bottom list which, for the **From everyone except** option, indicates the restricted recipient for the group.

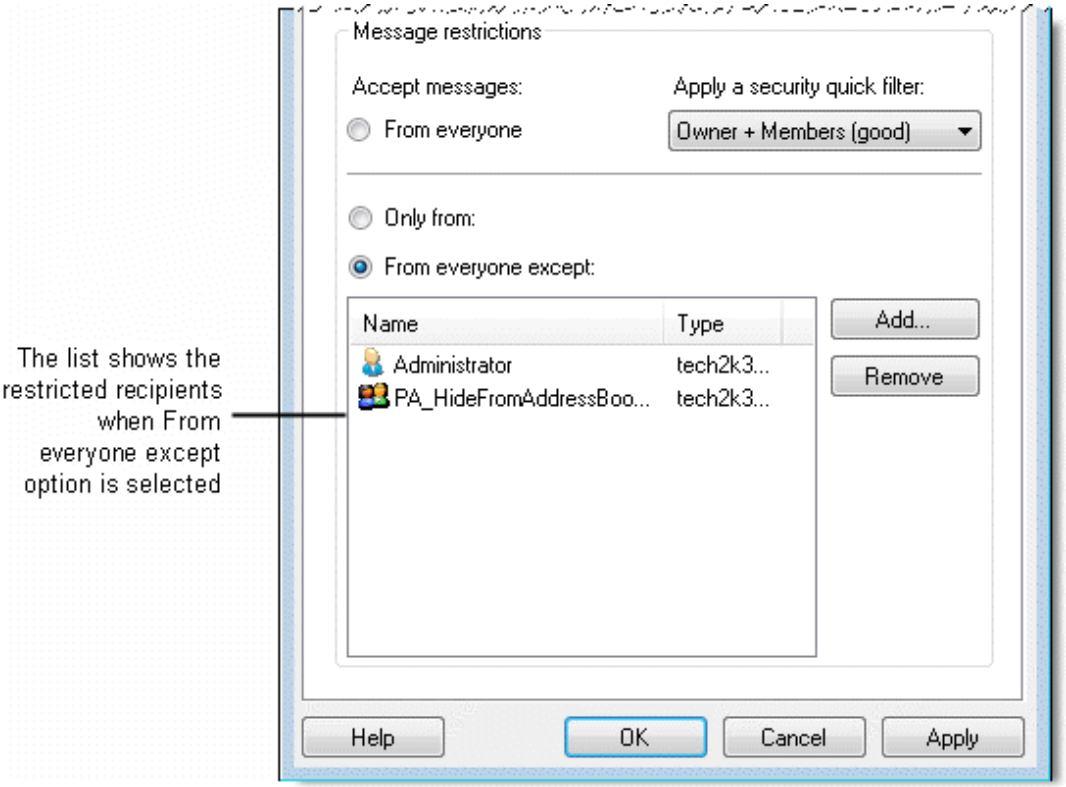


Figure - The list showing the restricted recipients

3. Click **OK**.

Selecting Expansion Server

The Expansion server is the Exchange server responsible for expanding a group and creating a message for each of the members. When a group is created, by default, it is set to use any available server in the organization for expansion. You can limit it to a specific server, if required.

Use the instructions below to select the server:

1. On the Properties dialog box of the group, click the **Exchange Advanced** tab.
2. Click **Browse** next to the **Expansion server** box and select the required server from the list. You can revert back to the default setting (that is, any server in organization) by clicking **Browse** and then clicking **OK** without selecting a server from the list.
3. Click **Apply**.

Hiding Group from Address Lists

You can prevent a mail-enabled group from appearing in Exchange address lists. Use the instructions below to hide a group:

1. On the Properties dialog box of the group, click the **Exchange Advanced** tab.
2. Select the **Hide group from Exchange address lists** check box.
3. Click **Apply**.

Hiding Group Membership from Address Book

Exchange settings of a mail-enabled group allow its members to be hidden from the Outlook address book. You can set it using the instructions below:

1. On the Properties dialog box of the group, click the **Exchange Advanced** tab.
2. Select the **Hide membership from address book** check box.
3. Click **Apply**.

Setting Group to Send Out-of-Office Message

You can set a mail-enabled group to send out-of-office auto-replies to the message originator, when a message is sent to the group and one or more of the group members have out-of-office status.

To apply this setting:

1. On the Properties dialog box of the group, click the **Exchange Advanced** tab.
2. Select the **Send out-of-office messages to originator** check box.
3. Click **Apply**.

Setting Recipient for Non-Delivery Reports

If a message sent to a group is not delivered, by default, nobody is informed about the delivery failure. You can change this setting to notify either the group owner or the message originator about the delivery failure by sending a non-delivery report.

To apply the setting:

1. On the Properties dialog box of the group, click the **Exchange Advanced** tab.
2. In the **Delivery reports** area:
    i. Click **Send delivery reports to group owner** or **Send delivery reports to message originator** to notify the group owner or message originator respectively about the delivery failure.
    ii. Click **Apply**.

Assigning Values to Custom Attributes of a Group

Exchange provides 15 custom attribute fields that you can use to add additional information about the object. For example, you can use custom attributes to save health insurance data of the manager of a mail-enabled group. To do this:

1. On the Properties dialog box of the group, click the **Exchange Advanced** tab.
2. Click **Custom Attributes**. This displays the **Exchange Custom Attributes** dialog box showing the list of all custom attributes.
    i. Select an attribute and click **Edit**. This displays another dialog box where you can type a value for the custom attribute.
    Repeat this step to add values for all custom attributes.

ii. After adding values for the required attributes, click **OK** to close the **Exchange Custom Attributes** dialog box.

3. Click **Apply** on the Properties dialog box.

Chapter 12: Dynasties

This chapter provides comprehensive information about Dynasties. Instructions on creating and managing Dynasties are also included. The chapter also introduces you with different customization and configuration option available for Dynasties.

The chapter is divided into following sections:

Dynasties, gives an overview of Dynasties and explains how they are structured.

Creating a Dynasty, provides instructions on creating a new Dynasty.

Dynasty, covers the customization options available for Dynasties.

Dynasty, describes global configurations that apply to all Dynasties.

Dynasties - Overview

A Dynasty is effectively a SmartGroup that creates and manages other SmartGroups based on each distinct value of the Active Directory attribute it is grouped by. The SmartGroups created by the Dynasty are called child groups and become members of their parent, which is called a Dynasty. Adding a group as a member of another distribution list is called nesting, so in this way Dynasties are layer of nested groups.

You may ask yourself how does a Dynasty determine when to create a child group? When a user creates a Dynasty, they specify a query and a field to group-by. The group-by field is used to divide the query results into groups. For example, if you specified to group the query results by the department field, then only each of the distinct values for department would be returned and a child group created: Sales, Marketing, Human Resources and so on.

Dynasty children inherits the characteristics and properties of their parents such as group type (in the case of Active Directory), group security, expiration policy, owner, delivery restrictions, message size restrictions and so on. This can save a considerable amount of time of creating groups separately and defining the properties for each.

Automate will keep the dynasty alive by adding new children as new values are returned by the group-by query and removing existing children as previous values disappear from the directory. This means that as new values of the department field appear, new groups are created and as old values disappear the corresponding child group is deleted. The same process occurs with the membership of each child group. When a user's department changes from sales to marketing it will remove them from the sales child group and add them to the marketing child group.

Even if you do not have reliable information in your Exchange server or Active directory, Dynasties can still be a life saver for you. Consider a sever distribution list - many organizations maintain a group for everyone on a particular server. While you can create a group effectively to have an accurate list you would still need to maintain and create a new groups for new servers that are commissioned and remove old groups for servers that were decommissioned. By creating a new Dynasty with a query to group-by the Home Server field, you create a solution that not only provides you with a group for each server that has mailboxes on it but you would also have a list that contains the entire Exchange organization because the children are all nested within the parent Dynasty.

Automate supports the ability to create multi-level Dynasties. For example, you can create one Dynasty to group-by Country, then State, and finally City. When updated, the Dynasty would create groups for everyone in a particular country that would then create a group for everyone in each state within the country, and finally it would create a group for each city within each state. Now you have a group for everyone within a country, state, and city and you never have to worry about them being out-of-date.

Automate's Dynasty feature provides a powerful method of creating and maintaining the larger dynamic distribution lists in your organization. When you use Automate with Active Directory, you gain the ability to create Dynasty security groups, which adds even more productivity. Dynasties are easy to experiment with because you can quickly delete all the children with a single click.

Creating a Dynasty

As explained earlier, Dynasty is a SmartGroup that has the capability to create and maintain the membership of other SmartGroups. A Dynasty retrieves data from Active Directory on the same pattern as SmartGroup, but it has its own mechanism of dividing the result set into child groups. Dynasty uses group-by field values to determine Dynasty levels, which will divide the query results into child groups.

Automate provides pre-defined Dynasty templates that is; Organizational, Geographical and Managerial that offers pre-defined group-by attributes for creating Dynasty levels. You can customize these templates or define your own group-by attributes to expand the Dynasty levels as per your requirements. You can also combine an external data source with the templates to provide extended criteria for determining the group's membership.

Use the instructions below to create a new Dynasty:

1. In the GroupID Management Console; expand the **Automate** node, right-click **All Groups**, point to **New** and then click **Dynasty**. This starts the **New Dynasty** wizard.

2. On the welcome page of the **New Dynasty** wizard, read the welcome message and click **Next**.

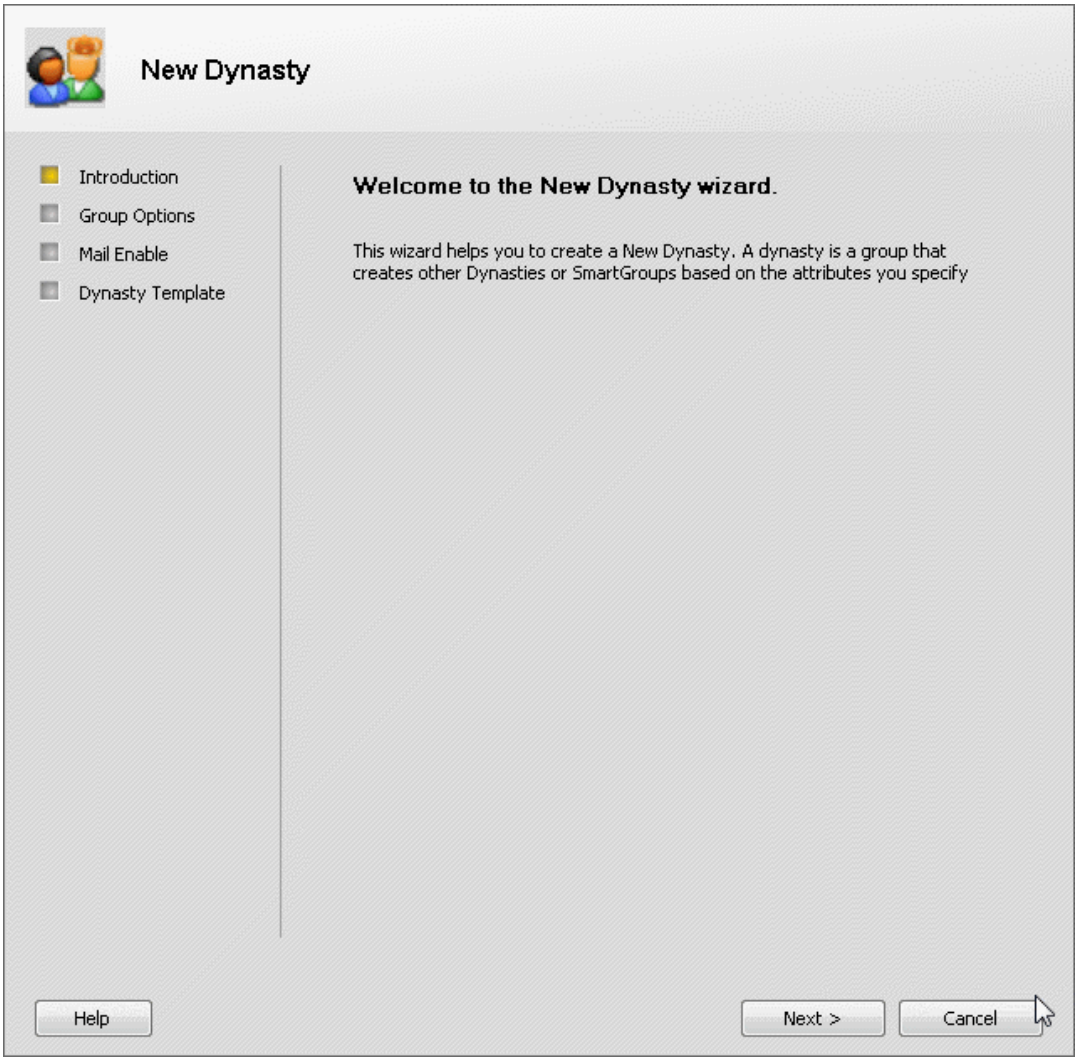

New Dynasty
Introduction
Group Options
Mail Enable
Dynasty Template
Welcome to the New Dynasty wizard.
This wizard helps you to create a New Dynasty. A dynasty is a group that creates other Dynasties or SmartGroups based on the attributes you specify
Help
Next >
Cancel

Figure - The welcome page

3. On the **Group Options** page:

   i. Click **Create in** to select the container in which to create the new group.

   ii. In the **Group name** box, type the name of your group.
   Your typed Group name is set by default for the **Group name (Pre-Windows 2000)** box. However, you can change this if required.

If prefixes are defined, the prefix list appears before the box from where you can select a prefix for the group. For information about prefixes, see **Group Name Prefixes** in **Part 7: GroupID Configurations**. After selecting the prefix; as you type the Group name, it shows the **Name Preview** including the prefix, below the box.

Figure - The prefixes list

iii. From the **Group Scope** area, select the required scope for the Dynasty. For information about group scope, see **Group Scope** in **Chapter 2: Group Management Concepts**.

iv. From the **Group Type** area, select whether this will be a security group or a distribution group. For information about group types, see **Group Types** in **Chapter 2: Group Management Concepts**.

v. From the **Group Security** list, select the required security type. For information about security types, see **Security Type** in **Chapter 2: Group Management Concepts**.

Requires Self-Service license

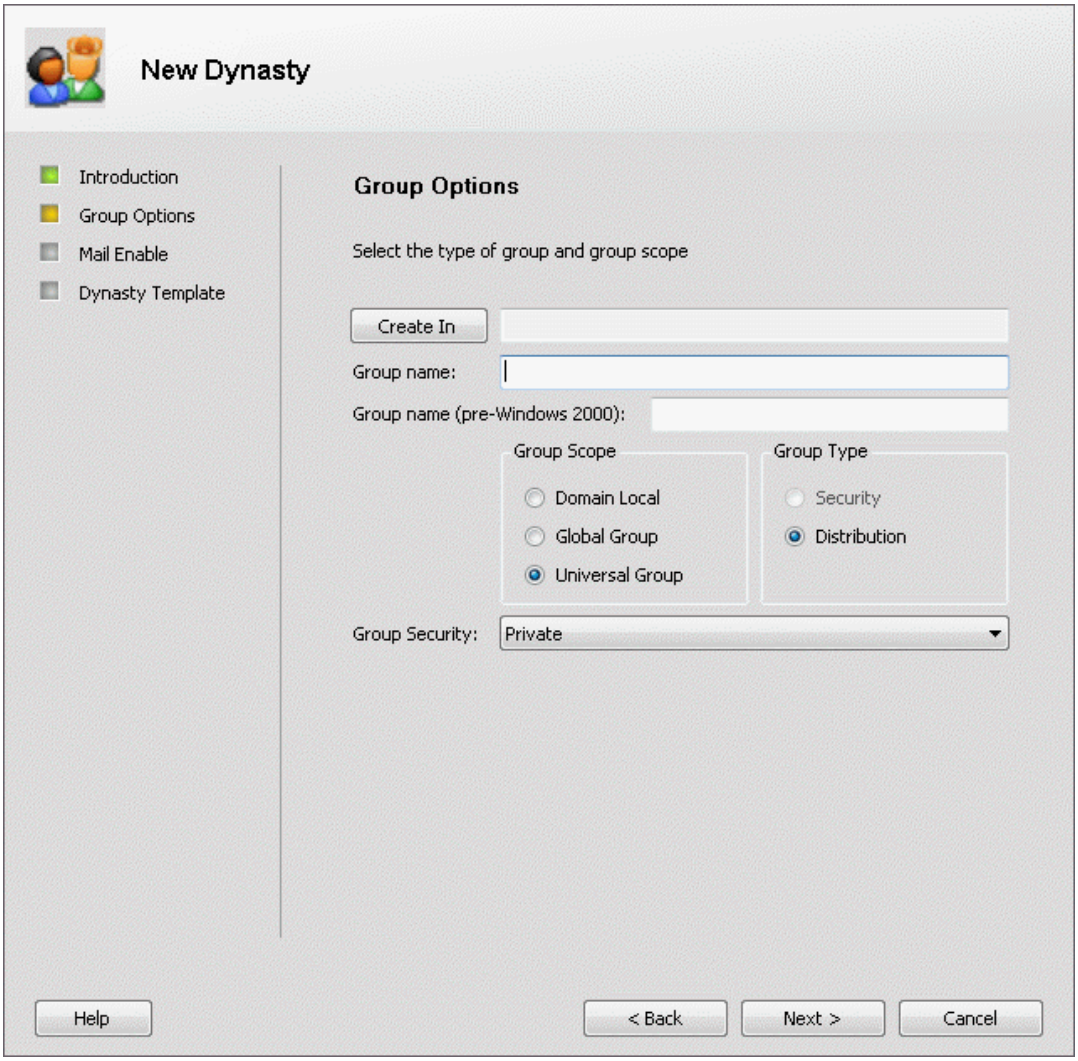


Figure - The Group Options page

4. Click **Next**.

5. By default, the **Create an Exchange e-mail address** check box is selected. On the **Mail-enable Group** page, you can change the alias and select an administrative group for the Dynasty.

If you do not want the Dynasty to be mail-enabled, simply clear the **Create an Exchange e-mail address** check box.

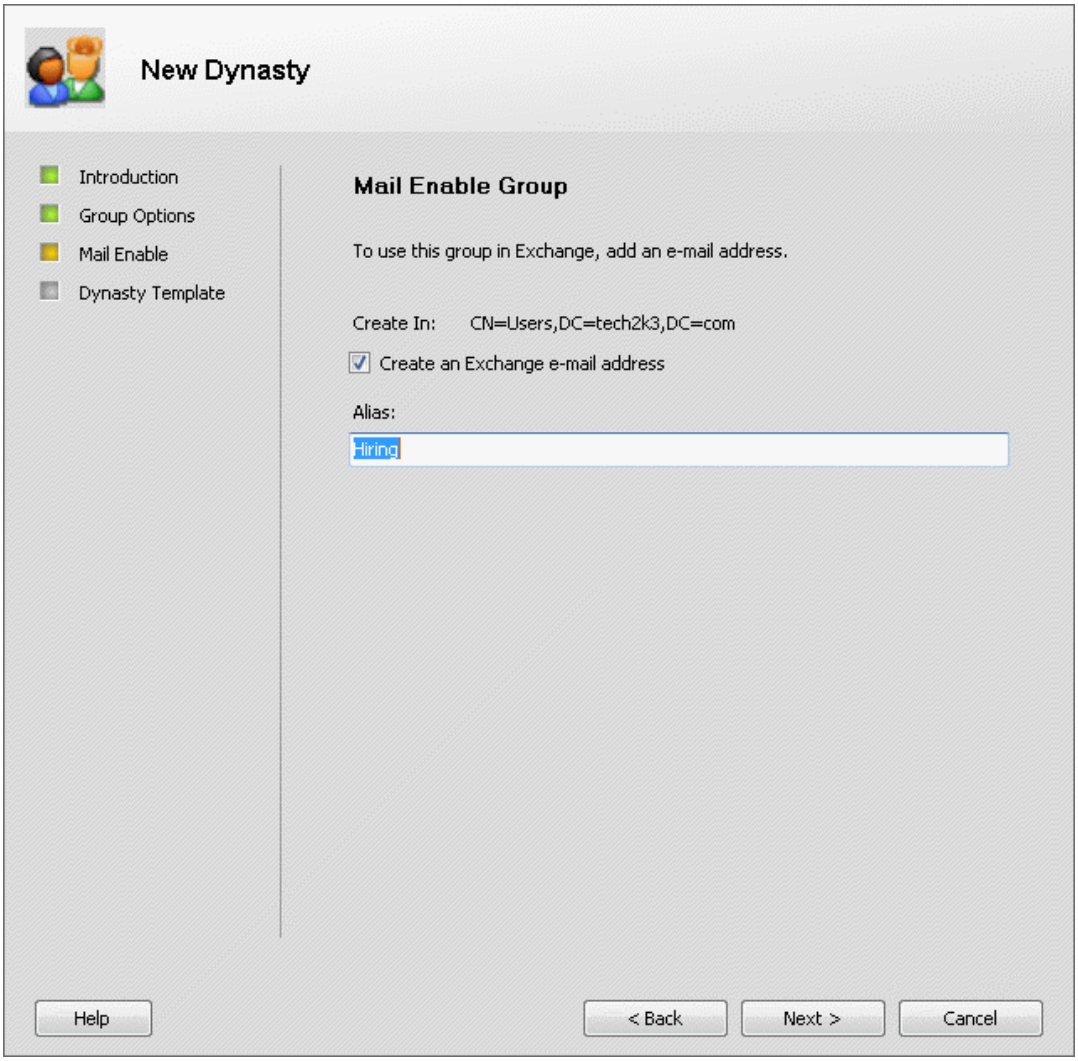


Figure - The Mail-enable Group page

6. Click **Next**.

7. The **Dynasty Templates** page provides you options either to select a pre-defined Dynasty template or select the group-by attributes of your choice. On this page:

    i. From the **Dynasty Templates** area, select:

        a. **Organizational**, to create group for every distinct company, then for each department within a company, and finally for each title in that department.

        b. **Geographical**, to create group for every distinct country, then for each state within a country, and finally for each city within that state.

        c. **Managerial**, to create group for all direct reports of a top manager, including the subordinates of the manager's direct reports.

        d. **Custom**, to begin with a blank group and select your own group-by attributes.

ii. You can combine an external data source with the group-by attributes to add an extra filter while determining the membership of child groups. For example, if you want to create an organizational Dynasty for all employees whose first names and last names are present in an external data source, you can select that data source and map its fields with the Active Directory fields. The New Dynasty wizard will filter only those users from Active Directory whose first names and last names match with the data source. To do this:

a. Select the **Database - Select database fields as Group By value** check box.

b. Click **Modify**. This displays the **Query Designer** dialog box where you can select the data source and configure the connection settings. For information about the data source configuration, see **Database Options** in **Chapter 13: The Query Designer**.

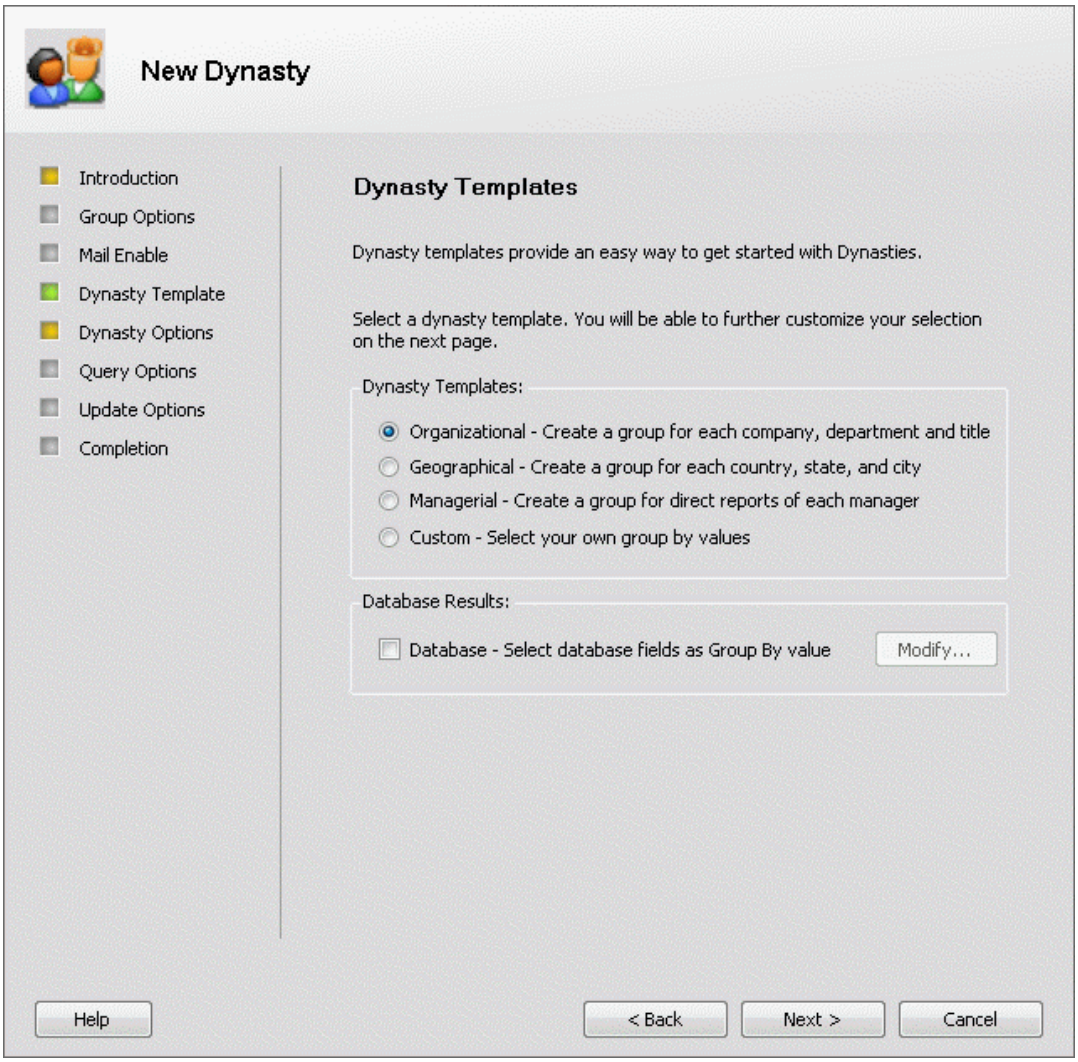

New Dynasty
Introduction
Group Options
Mail Enable
Dynasty Template
Dynasty Options
Query Options
Update Options
Completion
Dynasty Templates
Dynasty templates provide an easy way to get started with Dynasties.
Select a dynasty template. You will be able to further customize your selection on the next page.
Dynasty Templates:
Organizational - Create a group for each company, department and title
Geographical - Create a group for each country, state, and city
Managerial - Create a group for direct reports of each manager
Custom - Select your own group by values
Database Results:
Database - Select database fields as Group By value
Modify...
Help
< Back
Next >
Cancel

Figure - The Dynasty Templates page

8. Click **Next**.

9. The appearance of the **Dynasty Options** page depends on the Dynasty template selected on the previous page. If **Organizational** or **Geographical** template is selected, this page will show the list of default group-by attributes for the template. For **Custom** option, the page shows no attributes. You can manipulate this page to add or remove group-by attributes. To add a new group-by attribute:

    - Click **Add**. This displays the **GroupBy settings** dialog box where you can select the group-by field, change the child container (if required), apply group-by filters and provide separator for each group-by level.

    If **Managerial** template is selected on the previous page, the **Dynasty Options** page lets you select a Top Manager from where it constructs the Dynasty structure starting with creating a SmartGroup for all direct reports to the selected top level manager and continues down the Dynasty structure by creating SmartGroups for all direct reports to sub-level managers. On this page:

    i. Click **Top Manager** to select a top level manger to provide a starting location for the Dynasty.

    ii. By default, Managerial Dynasty structure adds sub-level manager's SmartGroups in the membership list of the top-level manager's SmartGroups. You can exclude them by selecting the **Exclude nested lists of direct reports** check box.

    iii. By default, Dynasty children are created in the same container as the manager being processed. To specify a different container or organizational unit for child groups, click **Create Groups in this container** and then click **Browse** to select the container.

    Figure - The Dynasty Options page when Custom template option is selected

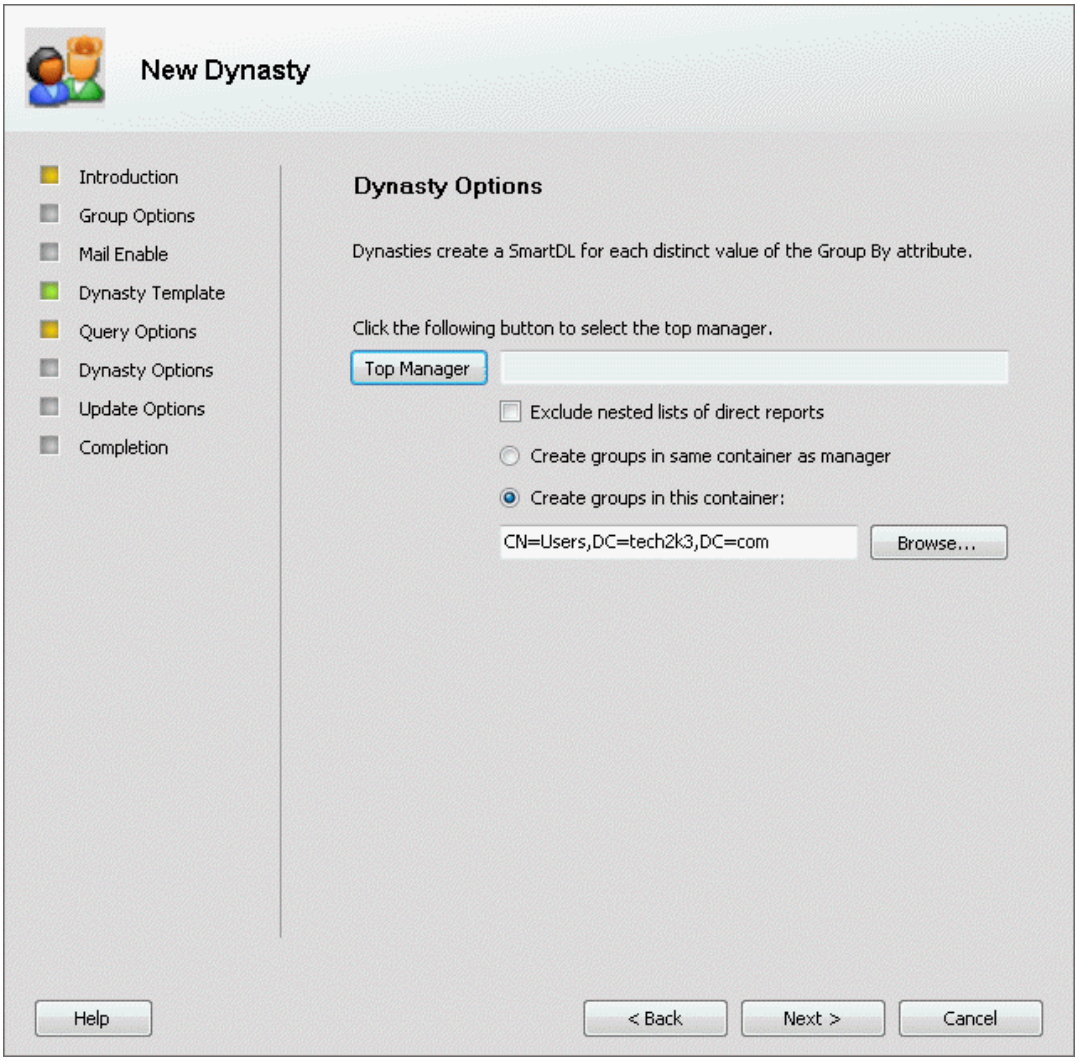


Figure - The Dynasty Options page when Managerial template option is selected

10. Click **Next**.

11. The **Query Options** page shows the default query for selecting the group members. The default query returns all users with Exchange mailboxes, users and contacts with external e-mail addresses, which are then grouped by the specified attributes. If external data source is specified, the query filters objects matching the values of the data source. You can click **Modify** to launch the Query Designer where you can edit the query. For information about the query designer, see **Chapter 13: The Query Designer**.

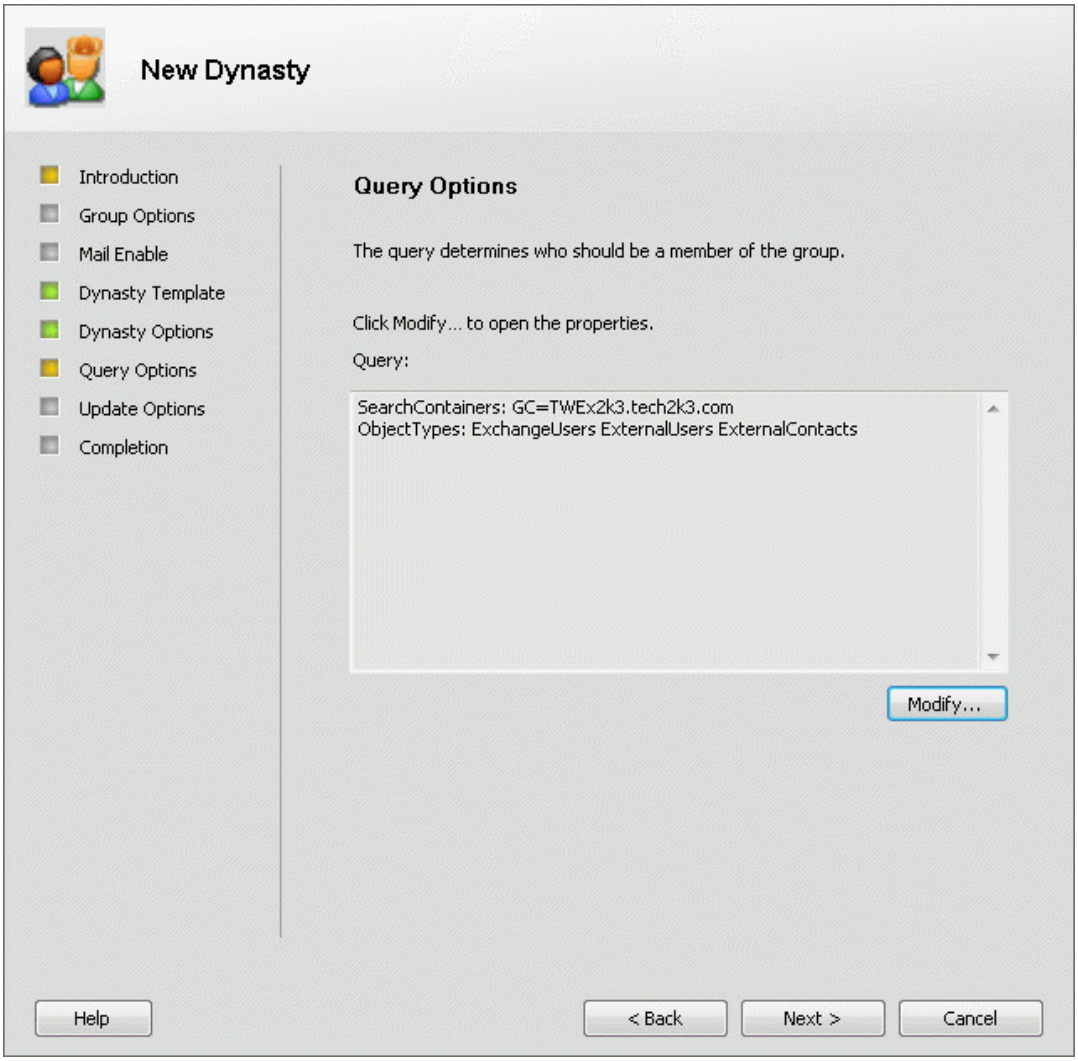


Figure - The Query Options page

12. Click **Next**.

13. On the **Update Options** page, select when you want to update the membership of the group. Following options are available:

    - **Now**, to update the Dynasty membership as soon as you click **Next**.
    - **Later, using the Update command or an existing job**, to manually update the membership of child groups later. This can be done by right-clicking the Dynasty and clicking **Update**. You can also apply a job schedule to the Dynasty later, if required.
    - **Later, using a new job on this machine**, to create a schedule to update Dynasty membership. Selecting this option enables the **SmartGroup Job** section where you can define the update schedule.

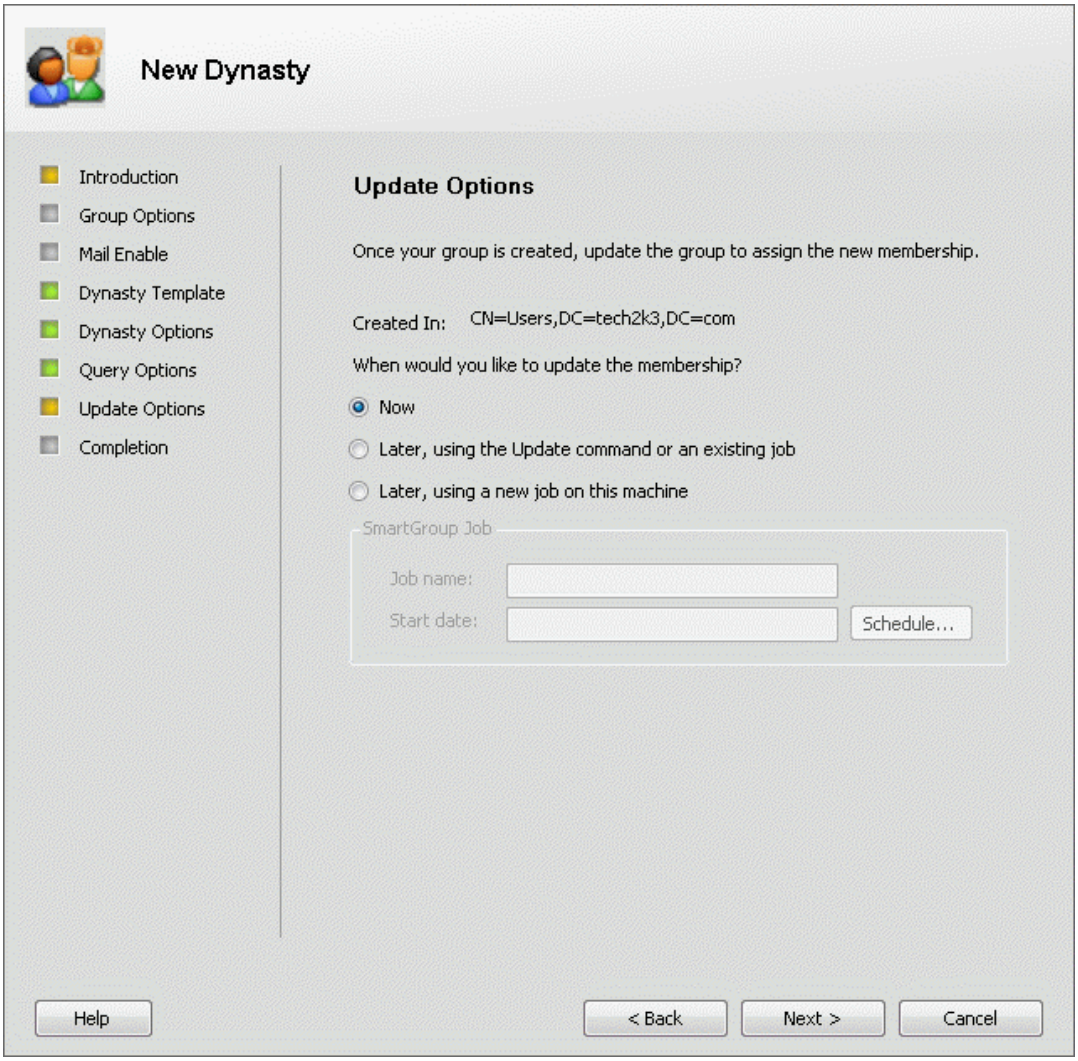


Figure - The Update Options page

14. Click **Next**.

15. On the last page of the wizard, click **Finish** and then click **Close** to create the Dynasty.

Dynasty Options

A Dynasty is essentially a SmartGroup so all features that a SmartGroup offers are also available for the Dynasty. You can update the membership of a Dynasty using the same procedures available for a SmartGroup. For more information about updating memberships, see **Updating Groups** in **Chapter 9: Managing Groups**. You can even schedule jobs to update Dynasty membership. For more information about job schedules, see **Scheduling** in **Chapter 9: Managing Groups**.

Besides these, Automate provides advance options which you can use to enhance the Dynasty structure and its membership. You can modify the group-by attributes for the Dynasty, edit the template of alias and display names and control the attributes inheritance to Dynasty children.

Managing Group-by Attributes

When you create a Dynasty, you provide group-by attributes on the basis of which the Dynasty structure is produced. You can change these group-by options later for any Dynasty level.

To do this:

1. Expand the **Automate** node, next expand the **All Groups** node and click **Dynasties**.
2. From the Dynasties list, right-click the required Dynasty and click **Properties**.
3. On the Properties dialog box, click the **GroupID** tab.
4. In the **Advance** area, click **Options**. This displays the **Dynasty Options** dialog box. On the dialog box:
    i. Click the **General** tab, if not already selected. This displays same options as available on the **Dynasty Options** page of the **New Dynasty** wizard. You can manipulate the tab by following the same instructions provided in **Creating a Dynasty** earlier.
    ii. Click **OK**.

These changes will be reflected on the next update of the dynasty.

Setting Attributes Inheritance

You can maintain a list of attributes globally that you want the children to inherit from their parent. For more information about maintaining the inheritance list, see **Setting Attributes to Inherit from Parent Dynasty** later in this chapter. By default, these attributes are inherited to children only when they are created. You can change this setting to always allow existing children to inherit whenever the parent's membership is updated. You can even set to omit the attributes list to be inherited to child dynasties.

To manage the attributes inheritance:

1. Expand the **Automate** node, next expand the **All Groups** node and click **Dynasties**.
2. From the Dynasties list, right-click the required Dynasty and click **Properties**.
3. On the Properties dialog box, click the **GroupID** tab.
4. In the **Advance** area, click **Options**. This displays the **Dynasty Options** dialog box. On the dialog box:
    i. Click the **Advanced** tab.
    ii. In the **Inheritance** area, select the required inheritance option:
        - **Inherit selected attributes only on creation,** to inherit the attributes list only when dynasty is created.
        - **Always inherit selected attributes**, to inherit the attributes list for every update.
        - **Never inherit selected attributes**, to skip the attributes in the list from inheriting to child dynasties.
    iii. Click **OK**.

These changes will be reflected on the next update of the dynasty.

Modifying Alias and Display Name Structure

You can provide templates for the alias and display name for the dynasty children. The default templates for different dynasties are as follows:

Dynasty Type	Alias Template	Display Name Template
Organizational, Geographical, Custom	*DynastyName*%GROUPBY%	*DynastyName*%GROUPBY%
Managerial	%MANAGER%directreports	Direct reports of %MANAGER%

%GROUPBY% is replaced with the actual value of the **group-by** field and **%MANAGER%** is replaced with the **displayName** of the manager being processed. If you wish to use an attribute other than displayName to name the child groups, update the %MANAGER% statement with the desired attribute name. For example, you can use manager's name attribute by updating the statement as %MANAGER.name%.

To modify templates:

1. Expand the **Automate** node, next expand the **All Groups** node and click **Dynasties**.
2. From the Dynasties list, right-click the required Dynasty and click **Properties**.
3. On the Properties dialog box, click the **GroupID** tab.
4. In the **Advance** area, click **Options**. This displays the **Dynasty Options** dialog box. On the dialog box:
    i. Click the **Advanced** tab.
    ii. To update the alias template, type in the new template in the **Alias template** box.
    iii. To update the display name template, type in the new template in the **Display name template** box.
    iv. Click **OK**.

These changes will be reflected on the next update of the Dynasty only when:
1) Alias (mailNickname) or displayname attributes are not added in the **Attributes to Inherit** list in the global configuration.
2) The attribute inheritance is not set to **Always inherit selected attributes**.
For information about attributes inheritance, see **Set Attributes Inheritance** earlier in this chapter.

Dynasty Settings

You can have complete control on how a Dynasty should be processed. You can force Dynasty to update its children when it is updated. You can set to delete Dynasty children when they are empty. You can also control the inherited attributes list for Dynasty when it creates children or when any of its child is updated.

Setting Dynasty Children to Update Automatically With Parent

When you update a parent dynasty (manually or the Automate service updates it according to the job schedule), by default, the membership of all its children are updated according to the changes in your Active Directory data.

You can control this setting manually by following the instructions below:

1. On GroupID Management Console, click **Configuration**.
2. Click **Modify System Configuration**. This displays the **Configurations** dialog box. On the dialog box:
    i. Expand **Client**, and then click the **Dynasties**.
    ii. In the **On dynasty update** area, select the **Update dynasty children** check box (if not already selected). You can clear this check box if you do not want dynasty children to be updated with their parents.
3. Click **OK**.

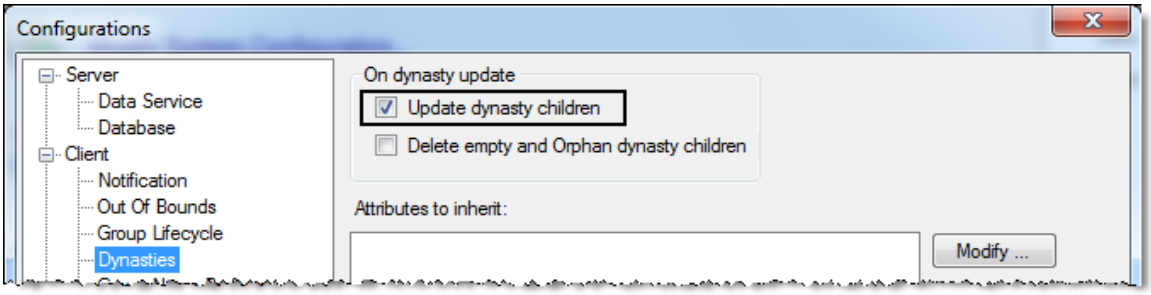


Figure - The Update dynasty children setting

Setting Empty and Orphan Dynasty Children to Delete Automatically

If by any reason, a child of a Dynasty has all of its members deleted or its parent Dynasty has been removed, it will remain in the directory as a useless group and may cause cluttering. Such child nodes of a Dynasty can automatically be deleted by applying the **Delete empty and Orphan dynasty children** setting. This will only affect the empty and orphan child nodes of a Dynasty and will not disturb its integrity and other functions.

> Remember, this setting does not delete the parent Dynasty.

Use the instructions below to apply this setting:

1. On GroupID Management Console, click **Configuration**.

2. Click **Modify System Configuration**. This displays the **Configurations** dialog box. On the dialog box:

    i. Expand **Client**, and then click **Dynasties**.

    ii. In the **On dynasty update** area, select the **Delete empty and Orphan dynasty children** check box (if not already selected). You can clear this check box if you do not want the orphan Dynasty children to be deleted automatically.

3. Click **OK**.

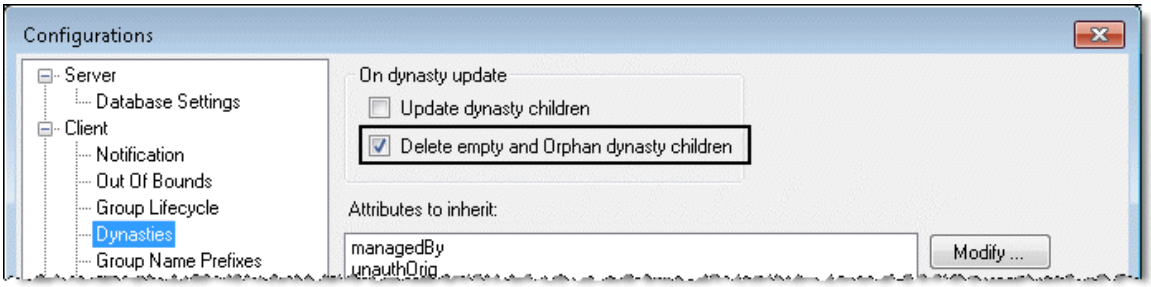


Figure - The Delete empty and Orphan dynasty children setting

Setting Attributes to Inherit from Parent Dynasty

Automate supports a concept known as Inheritance that is when a Dynasty creates children or when a child is updated, you can specify the attributes that the child should inherit from its parent. By default, following attributes of parent dynasty are inherited to children:

Attribute	Description
ManagedBy	Contains group owner information.
UnauthOrig	Contains the list of DNs of users who do not have permissions to send e-mail to the distribution group.
DLMemRejectPerms	Contains the DNs of groups that do not have permissions to send e-mail to the distribution group.
DLMemSubmitPerms	Contains the DNs of groups that have permissions to send e-mails to a specific group.
AuthOrig	Contains a list of DNs of users who have permission to send e-mail to the distribution group.
DelivContLength	Contains the maximum receive size limit.

You can select more attributes to inherit by following the instructions below:

1. On GroupID Management Console, click **Configuration**.

2. Click **Modify System Configuration**. This displays the **Configurations** dialog box. On the dialog box:

    i. Expand **Client**, and then click **Dynasties**.

ii. The **Attributes to inherit** list shows the attributes that are inherited from parent dynasty to the children. To add more attributes to this list:

- Click **Modify**. This displays the **Select Inheritable Attributes** dialog box. On the dialog box:

  a. From the **Inheritable attributes** list, select the attribute that you want to be inherited to the children.

  b. Click **Add**. This adds the attribute in the **Attributes to inherit** list. You can remove a attribute from the **Attributes to inherit** list by selecting it and clicking **Remove**.

  c. After adding the required attributes, click **OK** to close the dialog box.

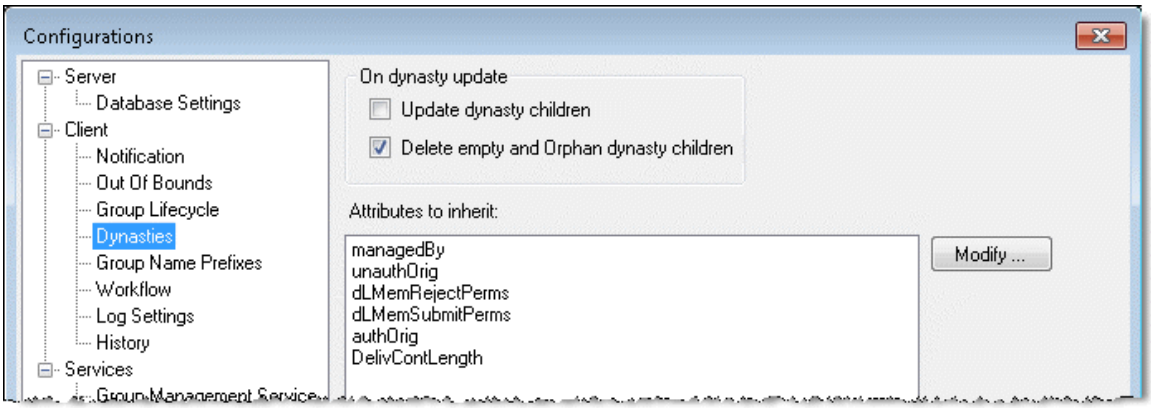


Figure - The Attributes inheritance area

Chapter 13: The Query Designer

The Query Designer allows you to create extremely complex LDAP queries with a very user-friendly designer interface. These queries provide a quick and consistent way to retrieve a common set of directory objects on which you want to perform specific tasks. For example, you can construct a query to retrieve all users having mailboxes on a particular Exchange server or you can build a query to retrieve all directory objects having their information present in an external data source; say, Microsoft SQL Server. The interactive options of the Query Designer allow you to query against multiple containers, with copy and paste, auto-complete, include/exclude and drag and drop support making it the most advanced Query Designer you can find for dynamic group management.

The Query Designer divides query options into six different tabs:

1. **General**, lets you select object categories that you want to find. For more information, see **General Query Options** later in this chapter.

2. **Password Expiry Options**, this tab is only available for **Password Expiry** groups and lets you define password expiration policies for a SmartGroup. For more information, see **Password Expiry Options** later in this chapter.

3. **Storage**, lets you filter the mailboxes to return. For more information, see **Storage Options** later in this chapter.

4. **Active Directory** lets you add additional filter criteria such as department, company, location and similar. For more information, see **Active Directory Options** later in this chapter.

5. **Advanced**, enables you to combine an external data source with Active Directory to determine a groups's membership. For more information, see **Database Options** later in this chapter.

6.

7. **Include / Exclude**, lets you include or exclude objects regardless of whether they are returned by the query or not. For more information, see **Include / Exclude Options** later in this chapter.

Launching the Query Designer

The Query Designer can be launched for a SmartGroup or a Dynasty using any of the following methods:

1. **While creating SmartGroup or Dynasty**

    - On the **Query Options** page of the New SmartGroup or New Dynasty wizard, click **Modify**.

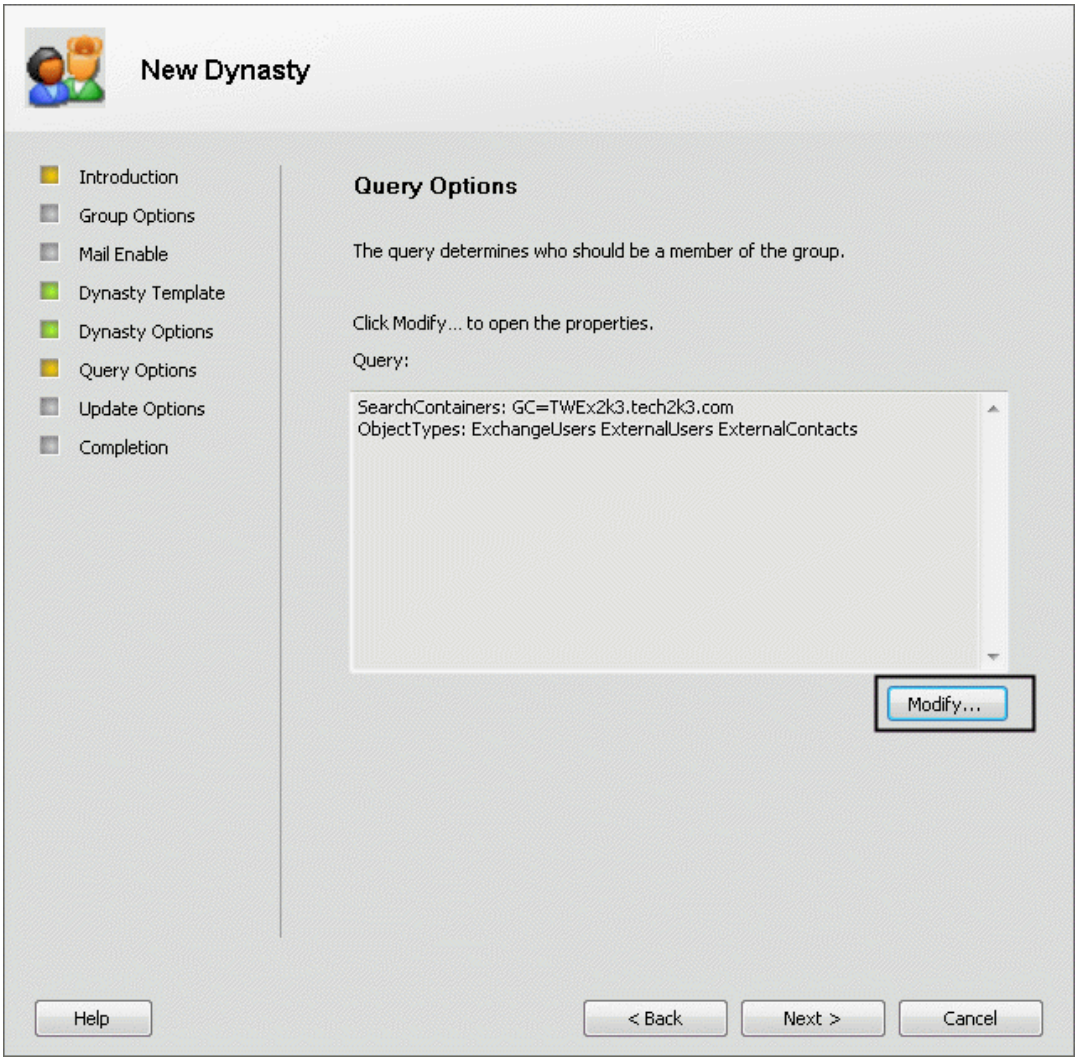


Figure - The Modify button on the Query Options page

2. **Using the shortcut menu**

   i. Click the **Smart Groups** or **Dynasties** node.

   ii. In the Groups list, right-click a SmartGroup or Dynasty and click **Modify Query**.

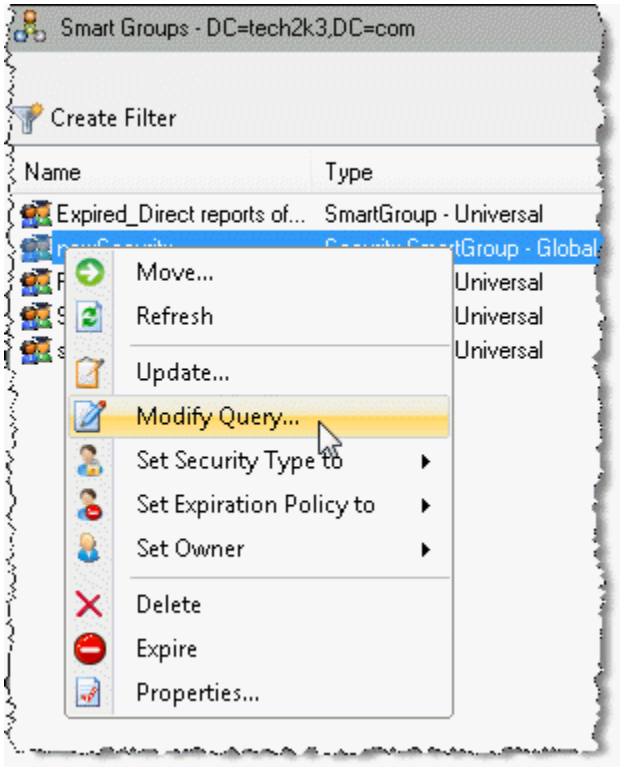


Figure - The Modify Query command on the shortcut menu

3. **From the Properties dialog box**

   i. Click the **Smart Groups** or **Dynasties** node.

   ii. In the Groups list, right-click a SmartGroup or Dynasty and click **Properties**.

   - On the Properties dialog box, click the **GroupID** tab.
     - In the **Query** area, click **Modify**.

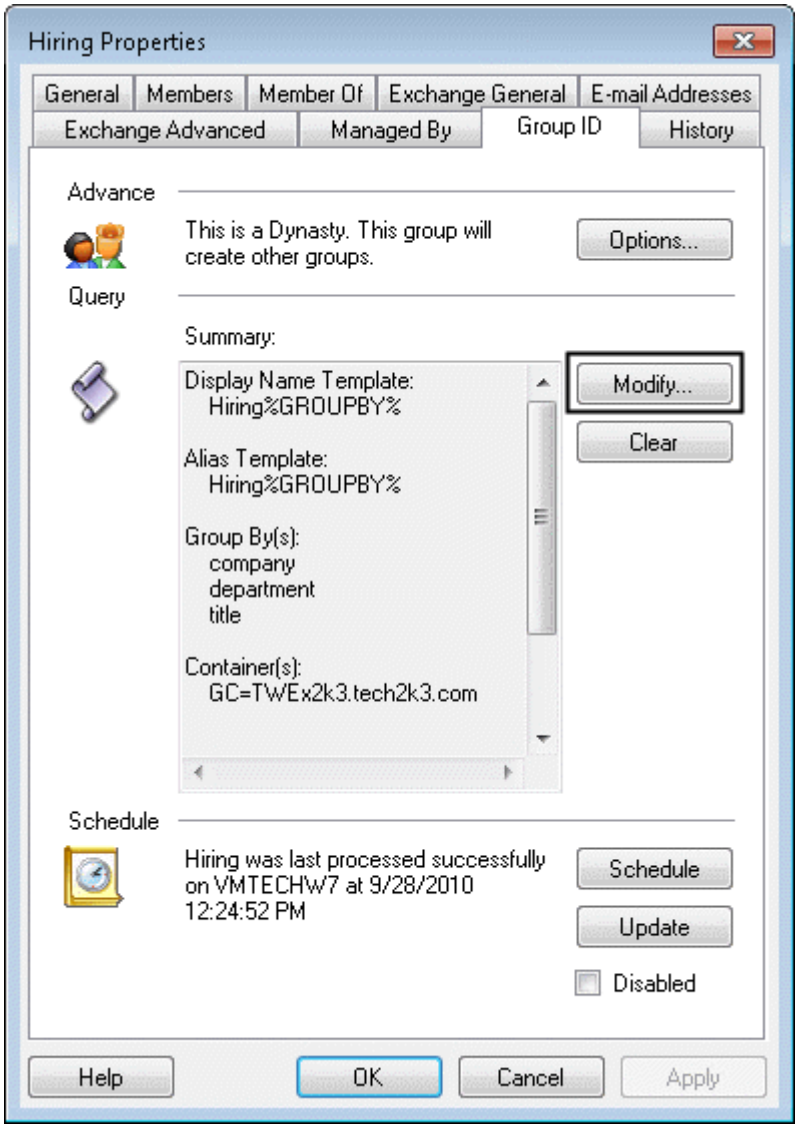


Figure - The GroupID tab of the Properties dialog box

General Query Options

The **General** tab of the Query Designer provides categorized options for filtering objects. The type of objects available on the tab depends on the option you have selected in the **Find** list. The table below shows different object categories on the General tab according to the option selected in the Find list:

Option in Find list	Description	Categories on the General tab
Exchange Recipients	Includes options to retrieve mail-enabled objects (Exchange 2003/2007).	• Users with Exchange mailboxes • Users with external e-mail addresses • Contacts with external e-mail addresses

Option in Find list	Description	Categories on the General tab
		• Mail-enabled Groups • Mail-enabled Public Folders
Computers	Includes options to retrieve Computers object only (Active Directory only).	• Workstations and Servers • Domain Controllers
Custom	Returns all objects regardless of **objectClass**. Be sure to add an objectClass predicate on the **Advanced** tab to avoid unpredictable results (Active Directory only).	• None
User, Contacts and Groups	Any user, contact, or group, regardless of whether they are mail-enabled (Active Directory only).	• User • Contacts • Groups

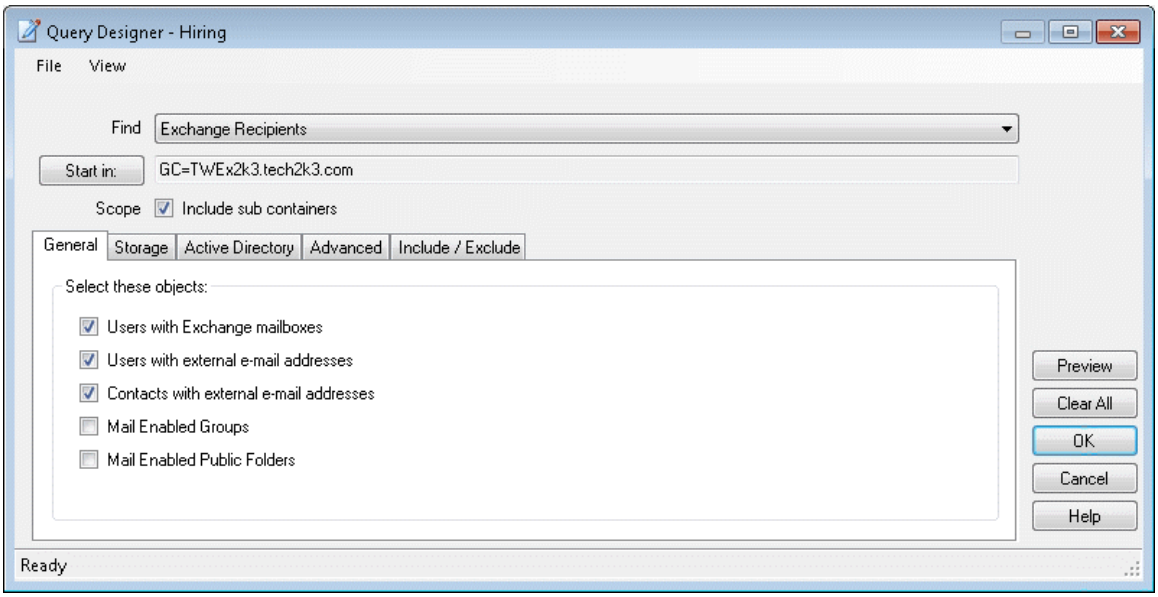


Figure - The General tab showing object types for the Exchange Recipients

Password Expiry Options

For Password Expiry groups, the Query Designer provides an extra tab where you can define the password expiration policy for the group. Based on the defined password, expiration policy and the users' **PWDLASTSET** attribute, Automate will automatically add users to the group whose password will soon expire and send them an e-mail notification. You can provide a template for the e-mail that you want to send to all members of the Password Expiry group when the group is updated. You can even include disabled users or users whose password never expire to the Password Expiry group.

Setting password expiry options for a Password Expiry group

1. Launch the Query Designer for the required group and click the **Password Expiry Options** tab.

2. In the **Domain Expiration Policy** box, type or select your maximum password age. The default is 42 days. Modifying the value in the Query Designer will not impact your domain security settings.

3. In the **Expiration Range Policy** box, type or select the expiration range. The expiration range determines when to include the user in the password expiry group. For example, a Domain Expiration Policy configured with a maximum password age of 30 days. Setting the Expiration Range Policy to 10 will include users in the Password Expiry group who have passwords aged 20 days or older.

4. You can select the **Include disabled users** check box to add disabled user accounts in the Password Expiry group, if required.

5. You can select the **Include users whose password never expires** check box to include users with the password never expires setting enabled, if required.

6. Select the **Send email after update** check box, if not already selected, to enable the group to send e-mail every time it updates its memberships.

   This feature is available once the group is created.

7. If you have selected the **Send email after update** check box, the **Email to Send** box will show the path of the default e-mail template that will be sent to all members of the group when it is updated. You can click **Browse** to select a different e-mail template.

8. Click **Find Now** to test which users match the given criteria.

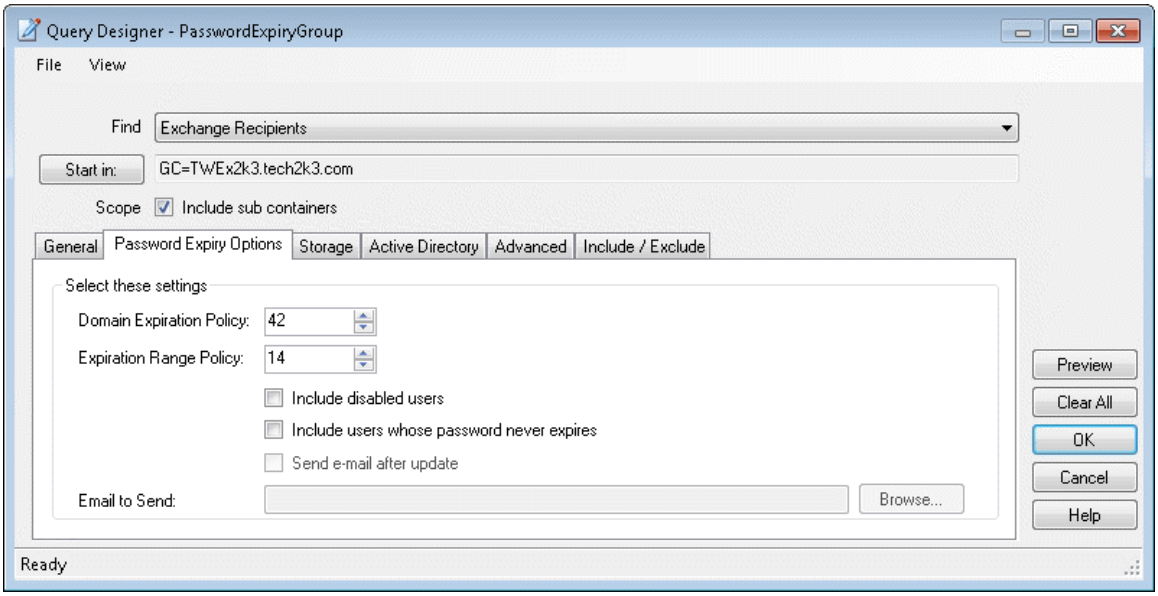


Figure - The Password Expiry Options tab

Storage Options

The default settings of the Query Designer retrieve all mailboxes irrespective of any server or mailbox store. You can apply filter to mailboxes you want the query to return. If filters are specified, the query will return only mailboxes on the specified server or mailbox store. This filter will not affect custom recipients, public folders, and distribution lists.

Add storage filters to the query

- Launch the Query Designer for the required group and click the **Storage** tab.

To filter mailboxes on a server

1. Click **Mailboxes on this server** and click **Browse**. This displays the **Select** dialog box where you can select the required server.
2. Click **OK** to close the dialog box.
3. Click **Find Now** to test which mailboxes match the given criteria.

To filter mailboxes on a mailbox store

1. Click **Mailboxes on this mailbox store** and click **Browse**. On the **Select** dialog box, select the required mailbox store.
2. Click **OK** to close the dialog box.
3. Click **Find Now** to test which mailboxes match the given criteria.

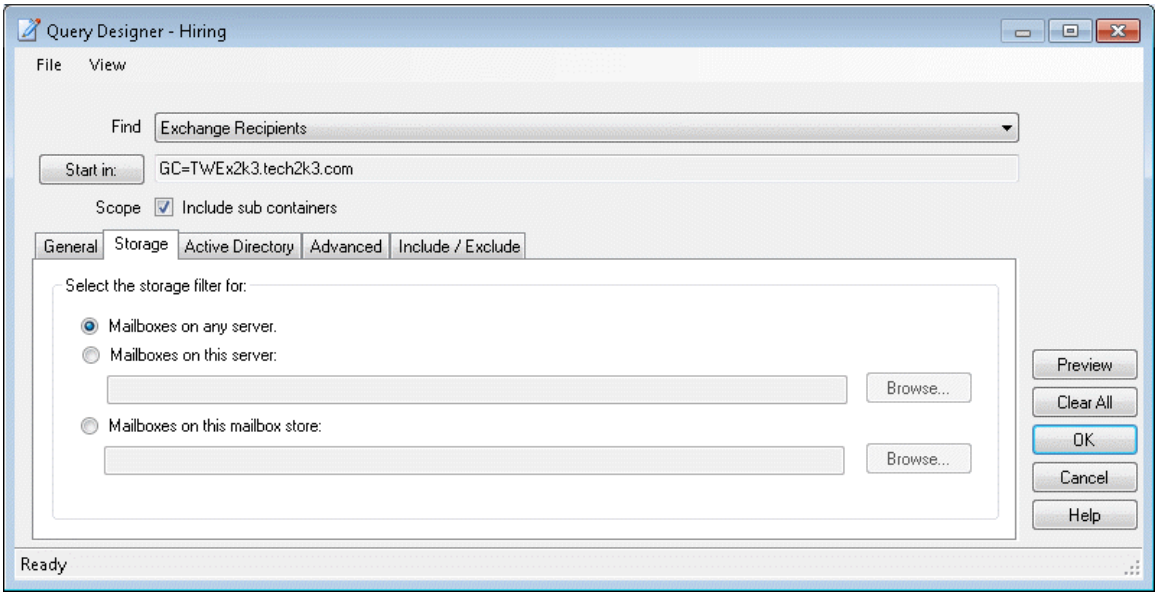


Figure - The Storage tab

Active Directory Options

You can add custom criteria to your query that does not fit in any option available on different tabs of the Query Designer. For example, you can add criteria to retrieve all directory users who live in Houston and they have a fax number. Interactive designer options let you apply logical operators (**AND**, **OR**) to your custom query to achieve the most accurate results. Cut, copy, paste, drag/drop and similar options are available to swiftly arrange the criteria according to your requirement.

Adding custom criteria to your query

1. Launch the Query Designer for the required group and click the **Active Directory** tab.

2. On the toolbar, click

.
This displays the **Add Criteria** dialog box.

3. On the **Add Criteria** dialog box:

    i. In the **Field** box, type or select the required field. The Field box contains attributes of Active Directory and Exchange (if installed on the server you are connected to).

    ii. In the **Condition** list, click the required condition that you want to apply to selected field. The table below shows the list of available conditions:

Condition	Description
Starts with	Returns everything that starts with the value.
Does not start with	Returns everything that does not start with the value.
Ends with	Returns everything that ends with the value (Note: this is resource intensive on the directory server).
Does not end with	Returns everything that does not end with the value (Note: this is resource intensive on the directory server).
Is (exactly)	Returns everything that matches the value.
Is not	Returns everything that does not match the value.
Contains	Returns everything that contains the value (Note: this is resource intensive on the directory server).
Not Contain	Returns everything that does not contain the value (Note: this is resource intensive on the directory server).
Present	Returns everything that has a value.
Not Present	Returns everything that does not have a value specified.
Greater than (>=)	Returns everything with a value greater than or equals to the given value.
Less than (<=)	Returns everything with a value less than or equals to the given value.

iii. In the **Value** list, type the value that determines whether it satisfies the criteria or not. For some operators the Value box will become unavailable, such as in the case of **Present** or **Not Present**. This is because these operators are not comparison operators. They only check if the value for the selected field exists or not and depending upon that return either true or false.

iv. Click **OK** to close the **Add Criteria** dialog box.

Following the procedure above, you can add multiple criteria to your query.

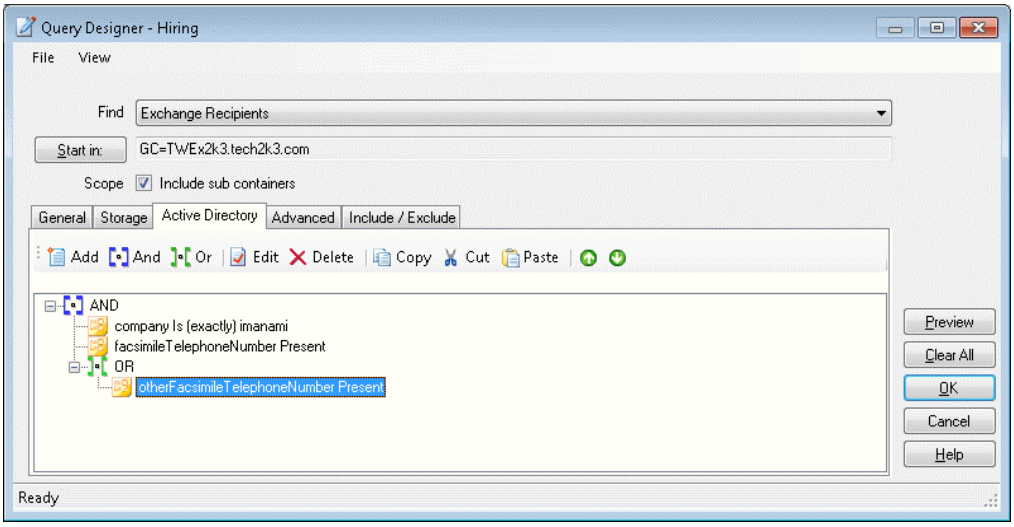


Figure - The Active Directory tab showing the custom criteria added

The toolbar options

The interactive toolbar available on the **Active Directory** tab helps you in adding, editing, deleting and arranging the criteria.

Toolbar Button	Keyboard Shortcut	Description
Add	INS	Opens the **Add Criteria** dialog box for adding a new criteria at the selected location.
And	CTRL + A	Inserts a logical AND to your criteria.
Or	CTRL + O	Inserts a logical OR to your criteria.
Edit	CTRL + ENTER	Opens the **Edit Criteria** dialog box that allows you to change the field, condition and value for the selected criteria.
Delete	DEL or SHIFT + DEL	Deletes the selected criteria.
Copy	CTRL + C	Copies the selected node to the clipboard.

Toolbar Button	Keyboard Shortcut	Description
Cut	CTRL + X	Cuts the selected node to the clipboard.
Paste	CTRL + V	Pastes a previously copied or cut node in the currently selected location.
	CTRL + UP	Moves the selected node one level up.
	CTRL + DOWN	Moves the selected node one level down.

Database Options

The Query Designer lets you combine an external data source with Active Directory to determine a groups' membership. The external data source can be Microsoft SQL server, ODBC data source, Oracle, text file and so on. You just need to provide the connection configurations and the Query Designer automatically connects to the data source using the given configurations and retrieves the results. It then queries Active Directory to find the matching records. You are required to map one or more columns retrieved from the data source with Active Directory attributes to join them. This mapping can be done using the **Active Directory** tab of the Query Designer.

Connecting to an external data source for retrieving members

1. Launch the Query Designer for the required group and click the **Advanced** tab.
2. Click **Modify** next to the **Connection** box. This displays the **Data Provider** dialog box where you can select the data provider and provide configurations for connecting to the data source.
3. As you select a data source on the **Data Provider** dialog box, the **Connection** box shows the connection string settings and the **Command** box shows the command the Query Designer executes to retrieve the query results from the data source. This can be a query statement and can include multiple columns separated by the comma character (,). The field names are enclosed in brackets ([ ]) to prevent any ambiguity the query engine might encounter because of spaces between column names. The columns included in the command statement are available on the **Active Directory** tab. Therefore, include the columns in the command statement that might be of use on the **Active Directory** tab.
4. Click **Execute** to execute the command and preview the results. This process may take time depending upon the size of your data source.

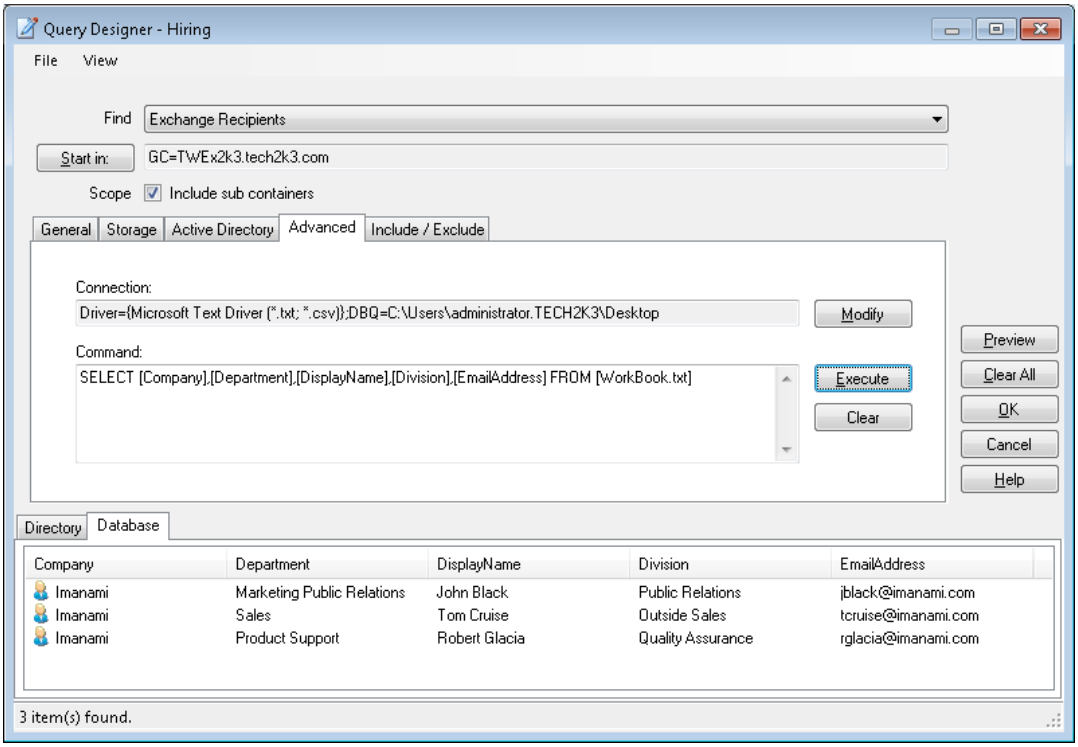


Figure - The Query Designer showing the results retrieved from external data source

Mapping data source with the Active Directory

1. On the Query Designer, click the **Active Directory** tab.

2. On the toolbar, click

. This displays the **Add Criteria** dialog box. On the dialog box:

    i. In the **Field** box, type or select the Active Directory or Exchange (if installed on the server you are connected to) attribute that you want to map with the data source.

    ii. In the **Condition** list, click the required condition.

    iii. In the **Value** list, click the required data source field. Data source fields appear in the Value list in the format: **Database.[*Data source field name*]**.

    iv. Click **OK** to close the **Add Criteria** dialog box.

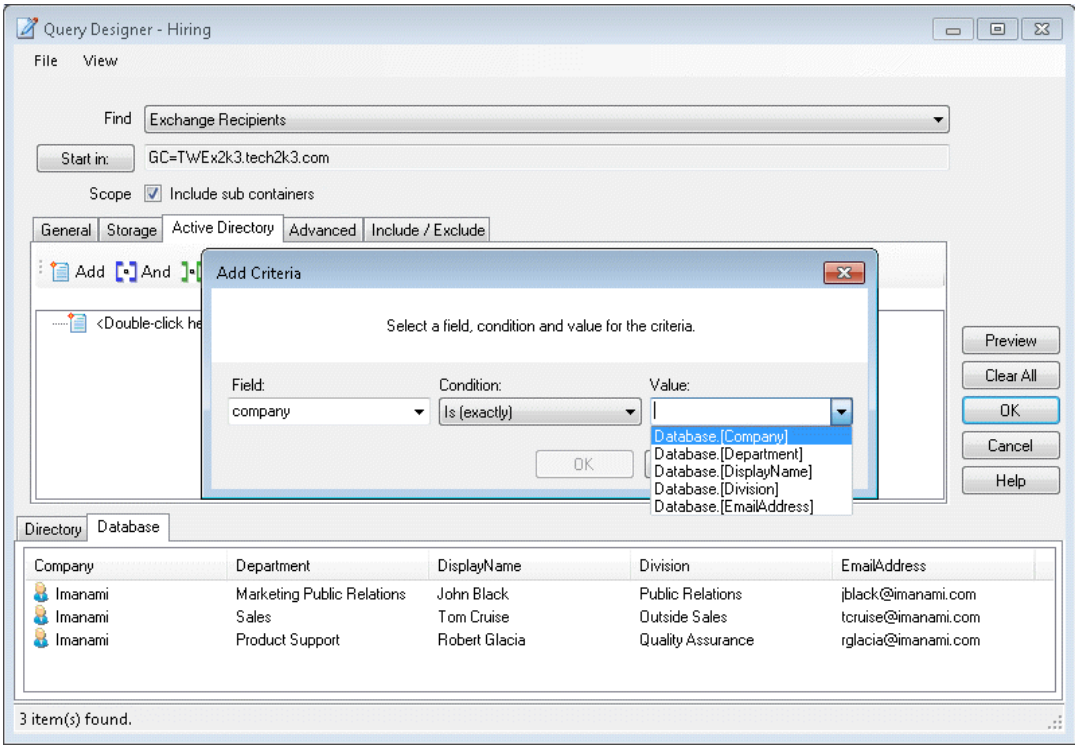


Figure - The Add Criteria dialog box showing the mapping of the Active Directory attribute with the data source field

Include / Exclude Options

You can include or exclude an object regardless of whether it is returned by the query or not. The include and exclude lists affect the group membership twice:

1. **Immediately**, as the Query Designer dialog box is closed, Automate adds the objects in the Include list to the group membership and removes the objects in the Exclude list from the group membership. If objects have been removed from the Include list, they will also be updated immediately. However, objects removed from the Exclude list will only be removed when the memberships of the group are updated interactively or by a scheduled job.

2. **On the group membership update**, as the group membership is updated either manually or by a scheduled job, Automate obtains the query results, then adds the objects to include and finally removes the objects to exclude.

For better performance, include or exclude objects using a criteria as opposed to statically selecting the objects using this tab.

Include an object to the query results

1. Launch the Query Designer for the required group and click the **Include / Exclude** tab.

2. In the **Include** area, click + Add. This displays the **Find** dialog box where you can search and select the required object. When you close the Find dialog box, the selected object displays in the Include area. You can remove an object from the Include area by selecting it and clicking ✕ Remove.

Following the same procedure as mentioned above, you can add/remove objects in the **Exclude** area that you want to exclude from the query results.

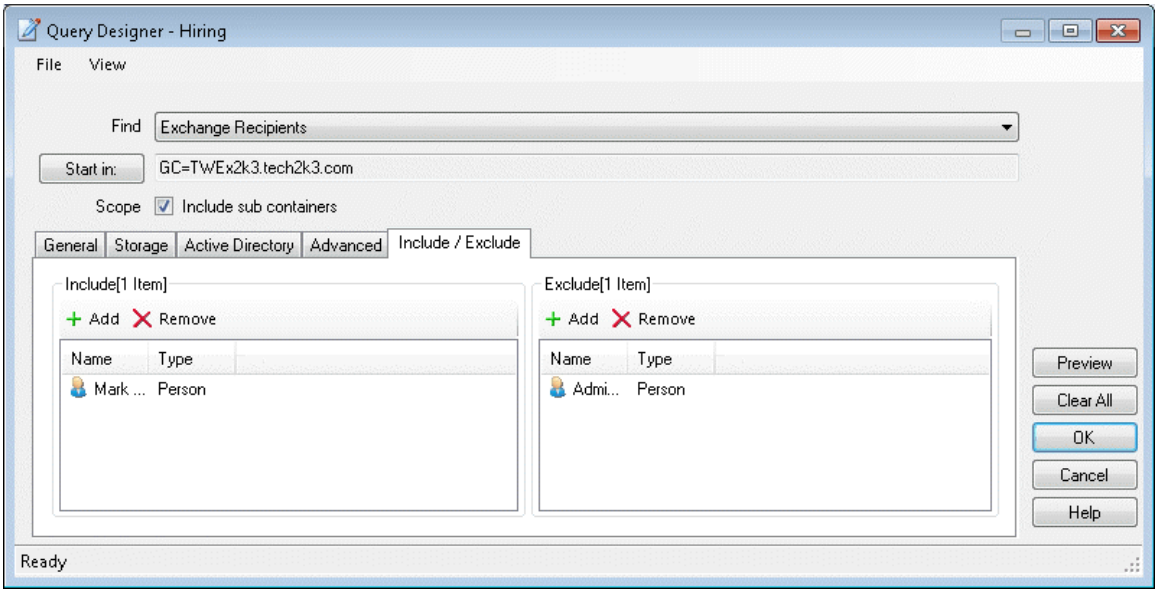


Figure - The Include / Exclude tab of the Query Designer

Part 4 - Synchronize

This part of the documentation covers the Synchronize module of GroupID. It explains how you can create a job to carry out data transfer. It also provides information on how you can apply different transformations while transferring data.

Chapter 14: Introduction, provides an overview of Synchronize, its key features and the user interface.

Chapter 15: Job Management, explains how you can create and manage Synchronize Jobs.

Chapter 16: Transformations, introduces you to transformations and its different types.

Chapter 17: Scripting, explains how you can build your own transformation script.

Chapter 18: Synchronize, covers the options available for different Synchronize settings.

Chapter 14: Introduction

This chapter provides an overview of Synchronize and its key features. It also helps you get familiarized with the module's user interface. The chapter is divided into the following sections:

Synchronize, provides a brief overview of Synchronize.

Features, describes the key features of Synchronize.

Getting Familiar with the User Interfaces, introduces you to the Synchronize user interface in the management console.

Synchronize - Overview

Synchronize is a set of technologies that allows you to transfer data from one data source to another. The data sources may include directory servers, databases or files. Synchronize supports a number of third party data sources and enables you to perform data transfers in between them.

Synchronize is also capable of applying transformations to the data being transferred. This allows you to convert data after retrieving it from the source and before it gets saved at the destination. The conversion can be simple, complex or custom. Synchronize provides a pre-defined set of transformation methods that you can apply to perform simple and complex conversions. Custom conversions are supported through VB.NET scripting. By writing conversion scripts using VB.NET, Synchronize users can extend the data transformation possibilities beyond those that are available out of the box.

Features

Support for Popular Data Sources

Synchronize supports a variety of popular data sources used in the industry today. These data sources include LDAP compliant directory services, relational database management systems, text files and spreadsheets. Synchronize also supports connectivity through ODBC (Open Database Communication) which makes it possible to connect to both relational and non-relational database management systems. The ODBC support also enables you to connect with data sources not originally supported by Synchronize out of the box.

Data Transformation

Transformations allow you to manipulate data before it gets saved to the destination. Use from five of the pre-defined Synchronize transformations, or write your own logic for complex data transformations using Visual Basic .NET.

Support for VB .NET

Synchronize provides support for Visual Basic .NET which is a full featured programming language for the Microsoft .NET framework. With this capability, you can extend Synchronize Jobs to any level you want.

Preview Results

View the results of your data transfer Jobs before actually making any changes to the data sources. The previewing feature lets you run and test a Job and review its results to make sure that they are as expected.

Scheduling

Schedule Jobs to run unattended daily, weekly, monthly or at any required frequency.

Job History

Synchronize maintains a history log for every Job. The history log provides the information about the dates and times the Job was run and its results.

E-mail Notifications

With e-mail notifications, receive a notification when a Job runs, fails or completes successfully.

Getting Familiar with the User Interface

In GroupID Management Console, the **Synchronize** node is shown below **Self-Service**. Unlike the other GroupID modules, the Synchronize node only has one sub-node that, on selection, shows the list of existing Jobs.

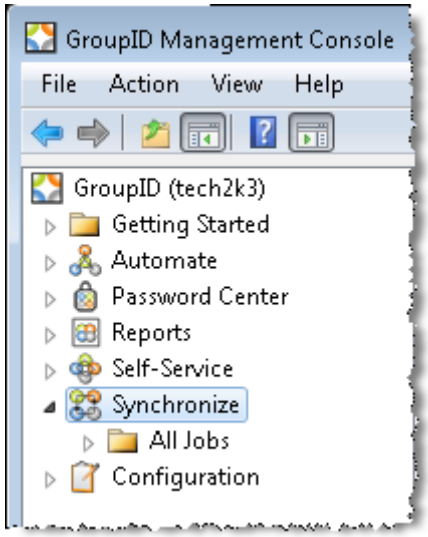


Figure - Points out Synchronize in GroupID.

The Job Run Chart

On selecting the **Synchronize** node, the right pane shows a bar chart of the recently executed Jobs. By default, the number of Jobs displayed on the chart are five. However, this can be changed using the options for Synchronize module. The horizontal axis (x-axis) shows the number of records that were processed in a job while the vertical axis (y-axis) shows the job names and the dates they were run. For jobs that fail, the chart displays the text **FAILED** instead of a bar. See the following figure.

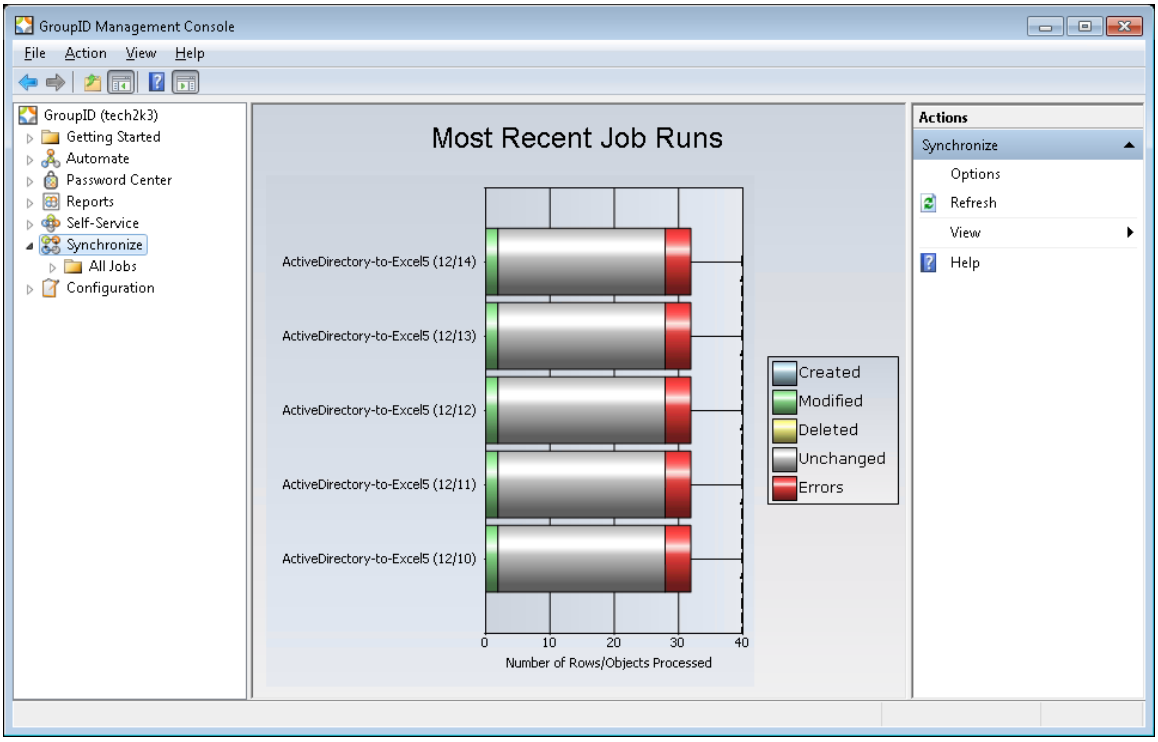


Figure - The right pane showing the graph of the recently run five Jobs.

The All Jobs View

This view is available by clicking the **All Jobs** node in the tree view. It lists all the existing Jobs and this will also be the place where you can modify these Jobs or create new ones.

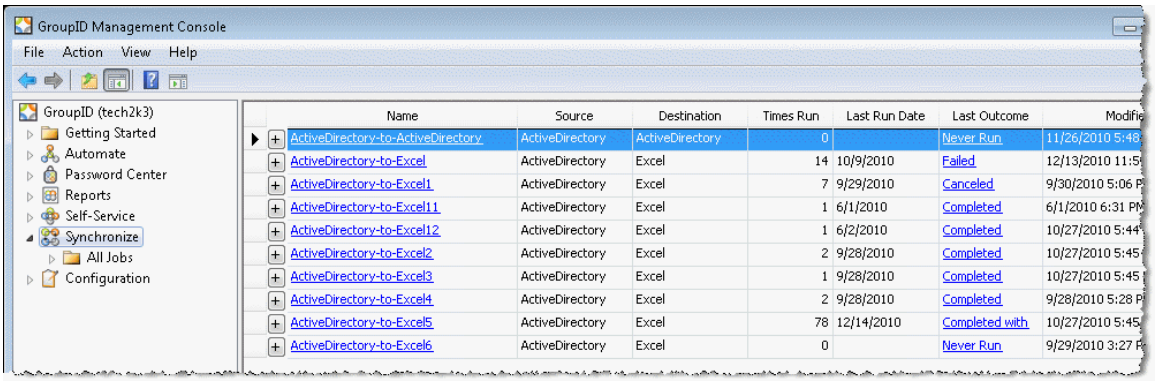

GroupID Management Console
File Action View Help
GroupID (tech2k3)
Getting Started
Automate
Password Center
Reports
Self-Service
Synchronize
All Jobs
Configuration
Name Source Destination Times Run Last Run Date Last Outcome
ActiveDirectory-to-ActiveDirectory ActiveDirectory ActiveDirectory 0 Never Run
ActiveDirectory-to-Excel ActiveDirectory Excel 14 10/9/2010 Failed
ActiveDirectory-to-Excel1 ActiveDirectory Excel 7 9/29/2010 Canceled
ActiveDirectory-to-Excel11 ActiveDirectory Excel 1 6/1/2010 Completed
ActiveDirectory-to-Excel12 ActiveDirectory Excel 1 6/2/2010 Completed
ActiveDirectory-to-Excel2 ActiveDirectory Excel 2 9/28/2010 Completed
ActiveDirectory-to-Excel3 ActiveDirectory Excel 1 9/28/2010 Completed
ActiveDirectory-to-Excel4 ActiveDirectory Excel 2 9/28/2010 Completed
ActiveDirectory-to-Excel5 ActiveDirectory Excel 78 12/14/2010 Completed with
ActiveDirectory-to-Excel6 ActiveDirectory Excel 0 Never Run

Figure - The All Jobs view

The right pane lists all the existing Jobs in a grid-like display. You can sort these items or group them based on the values of specific columns. You can also customize the view by selecting the columns that you would like to see for a Job.

To view the history of a Job, click the plus "+" button to the left of its name. This expands the item to display the history log of the job.

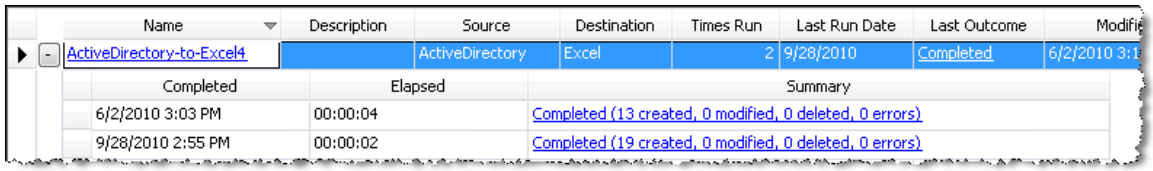


Figure - Shows the history information for the selected Job.

Similar to the Jobs view, you can also customize the columns displayed for the Job history.

Sorting the Jobs list

1. In the GroupID tree view, select the **All Jobs** node.
2. Click on the name of the column by which to sort the list. Clicking once will sort the list items in ascending based on the value of the selected column.
3. Click the same column again to sort the items in descending.

Chapter 15: Job Management

In this chapter you will learn how to work with Synchronize Jobs. A Synchronize Job is created to carry out a data transfer and transformation operation. Every Job has several settings associated with it which determine the data sources between which it is to transfer data, the field mappings, data conversions, notifications, scheduling, logging and more.

Creating a Job, takes you through the New Job wizard for creating a new Job.

Password Policy Validation, states how Synchronize validates static passwords.

Previewing Jobs, describes how to review the results of a Job without actually running it.

Running Jobs, provides instructions on how to execute a Job.

Synchronize, explains how you can run a synchronization job using the Windows command prompt.

Scheduling, provides instructions on how to schedule a Job.

Job Files, explains in detail the different files created for a Job and where they are located.

Logging Job Run Activities, explains the use of logging and its different levels.

Creating a Job

The New Job wizard simplifies the process of creating a Job in Synchronize. Before creating a new Job, it is a good practice to note down the following information in advance so that you don't have to face any inconvenience while creating the Job.

- Identify the source and destination data providers and any credentials that you may need to connect to them.
- Identify the fields that you need to copy from the source to destination.
- Identify any difference in the display or actual names of the short listed fields at the destination side.
- See whether any data transformation may be required.
- Will this Job be required to run once, or frequently?

Once you have identified the requirements based on the above given points, use the following instructions to create your new Job:

1. Expand the **Synchronize** node, right-click **All Jobs**, and then click **New Job**.
   This starts the **New Job** wizard.

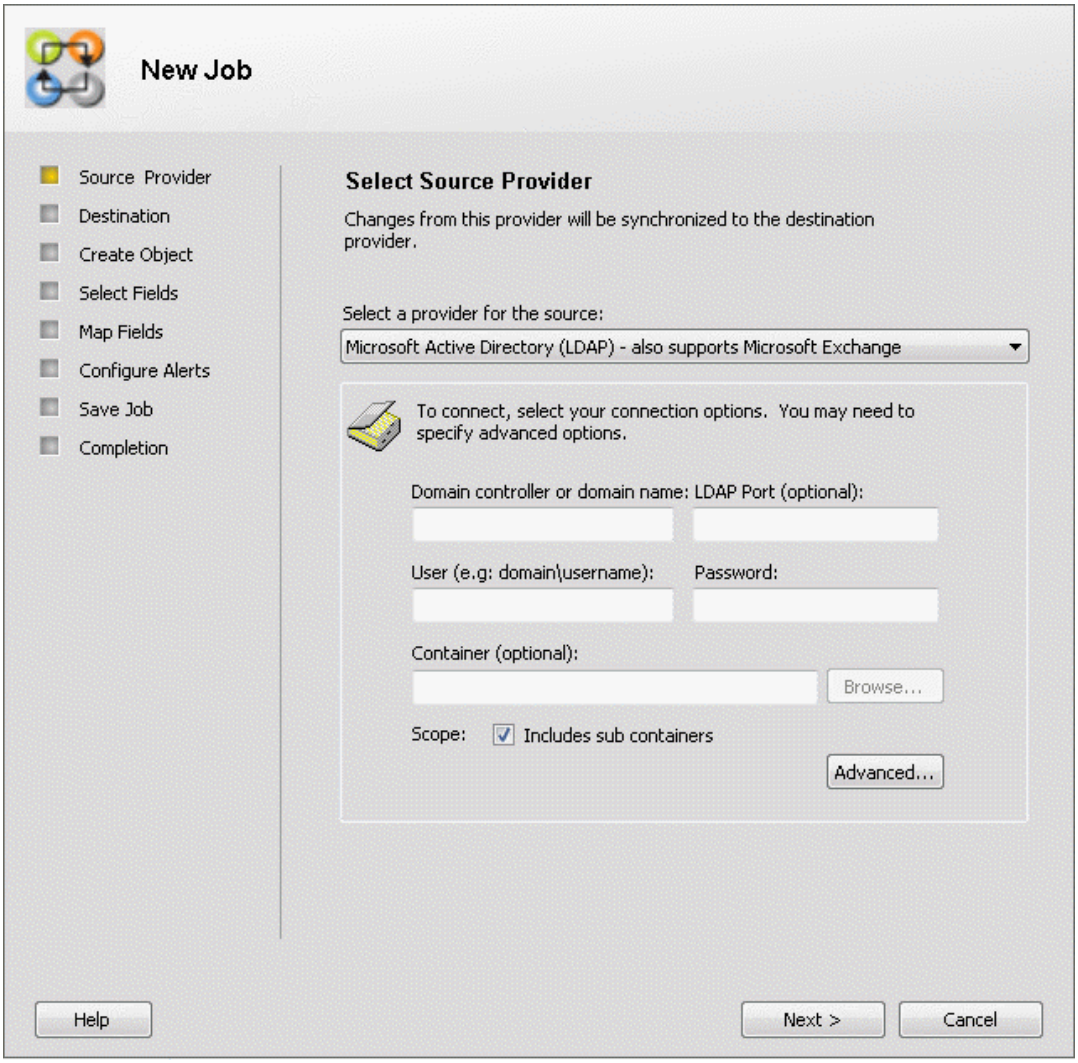


Figure - The opening page of the New Job wizard.

2. The opening page of the wizard requires you to configure the settings for the source to connect with.

    i. Select the required source provider from the **Select a provider for the source** list. Depending on your selection, the fields shown in the settings area will change based on information required to connect to the selected data source.

    ii. Enter the required information in the given fields and click **Next**.

3. The next page **Select Destination Provider** is similar to the previous one with the only difference that here you need to specify the settings for the destination provider where you would like to move data. On this page:

    i. Select the required source provider from the **Select a provider for the destination** list.
    Depending on your selection, the fields shown in the settings area will change based on information required to connect to the selected data source.

    ii. Enter the required information in the given fields and click **Next**.

4. On the **Create Object** page, specify if you would like to create a new object for every source object that does not already exist at the destination. If you do not choose to do so, the Job will only make updates to the existing objects at the destination.

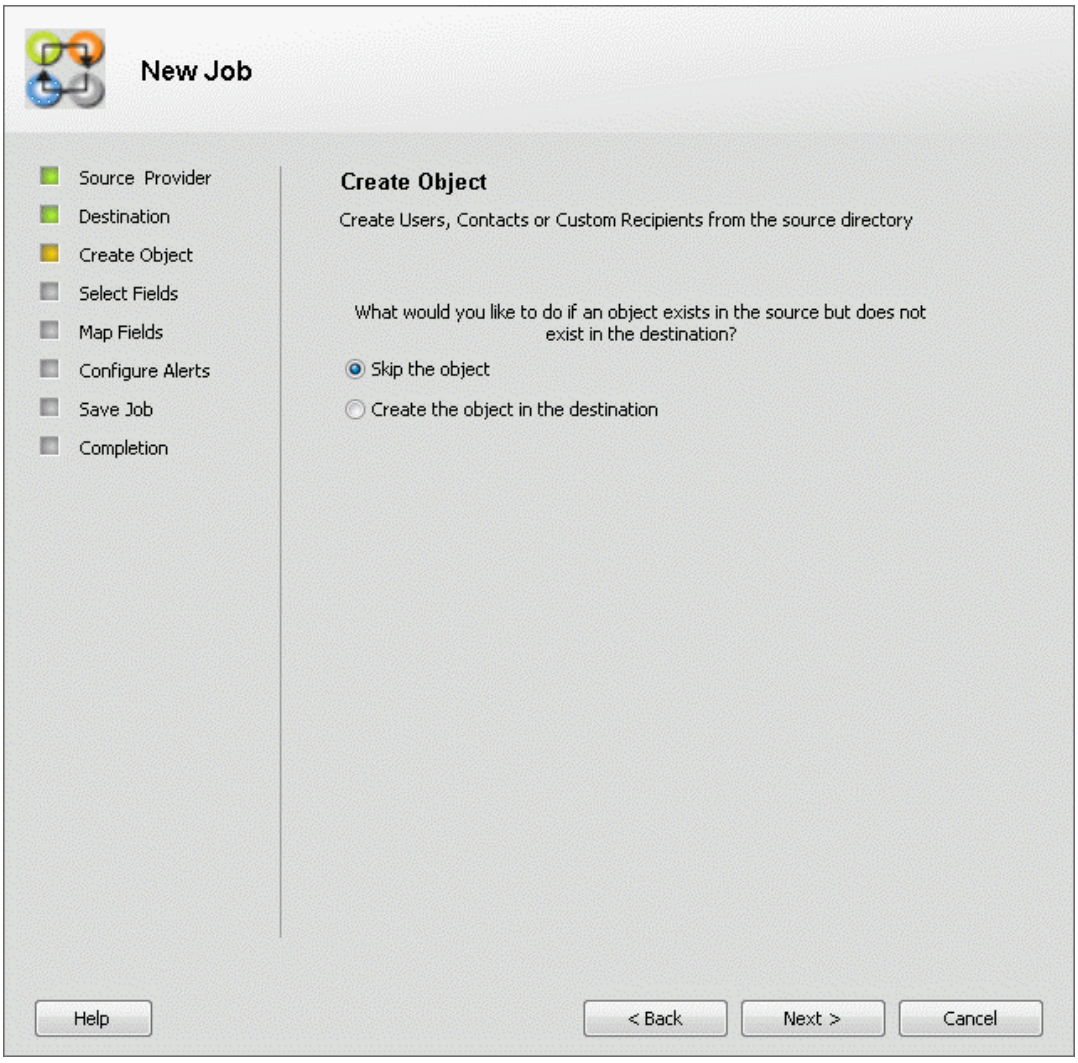


Figure - The Create Object page.

On this page, select:

- **Skip the object**, (default selection) to skip the creation of new objects and have the Job update only those that are already existing in the destination.
- **Create the object in the destination**, to create new objects at destination for those that do not already exist and update object that exist, if needed. If the destination data source is a directory service, such as Active Directory, the following additional settings will also have to be set:

    i. From the **What kind of object should be created** list, select the Active Directory object to create.

    ii. Depending upon the location in Active Directory where you want to create the new objects, select from one of the following:

- **Create objects in this container**, to set the container from the destination directory in which you want to create the new objects.
- **Create objects in the container specified in this source field**, to set the name of the field from the source containing the container name which Synchronize should use for creating the objects.
- **Create objects in a container specified in script**, to provide a custom logic through a script for Synchronize to determine the container in which it should create the new objects. Selecting this option enables the **Edit Script** button. Click this button to open the editor and write the script for your custom logic. To learn how to interact with the editor, refer to the topic **The Script Editor** in **Chapter 17: Scripting**.

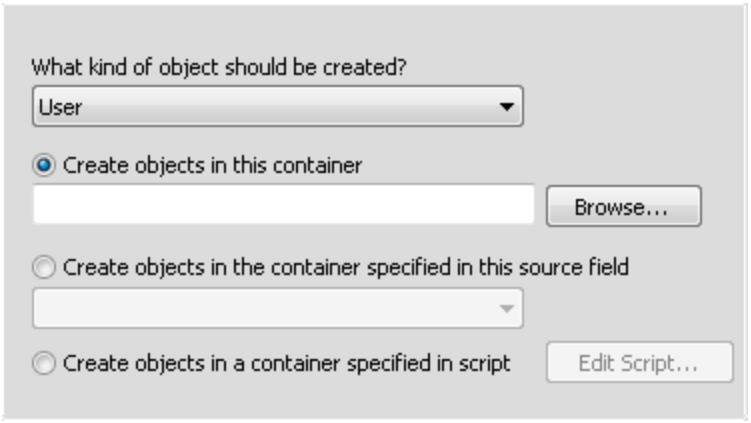

What kind of object should be created?
User
Create objects in this container
Browse...
Create objects in the container specified in this source field
Create objects in a container specified in script
Edit Script...

Figure - Additional Create Object settings available for directory services.

5. Click **Next**.
6. On the **Select Destination Fields** page, select the fields from destination that you want to synchronize.

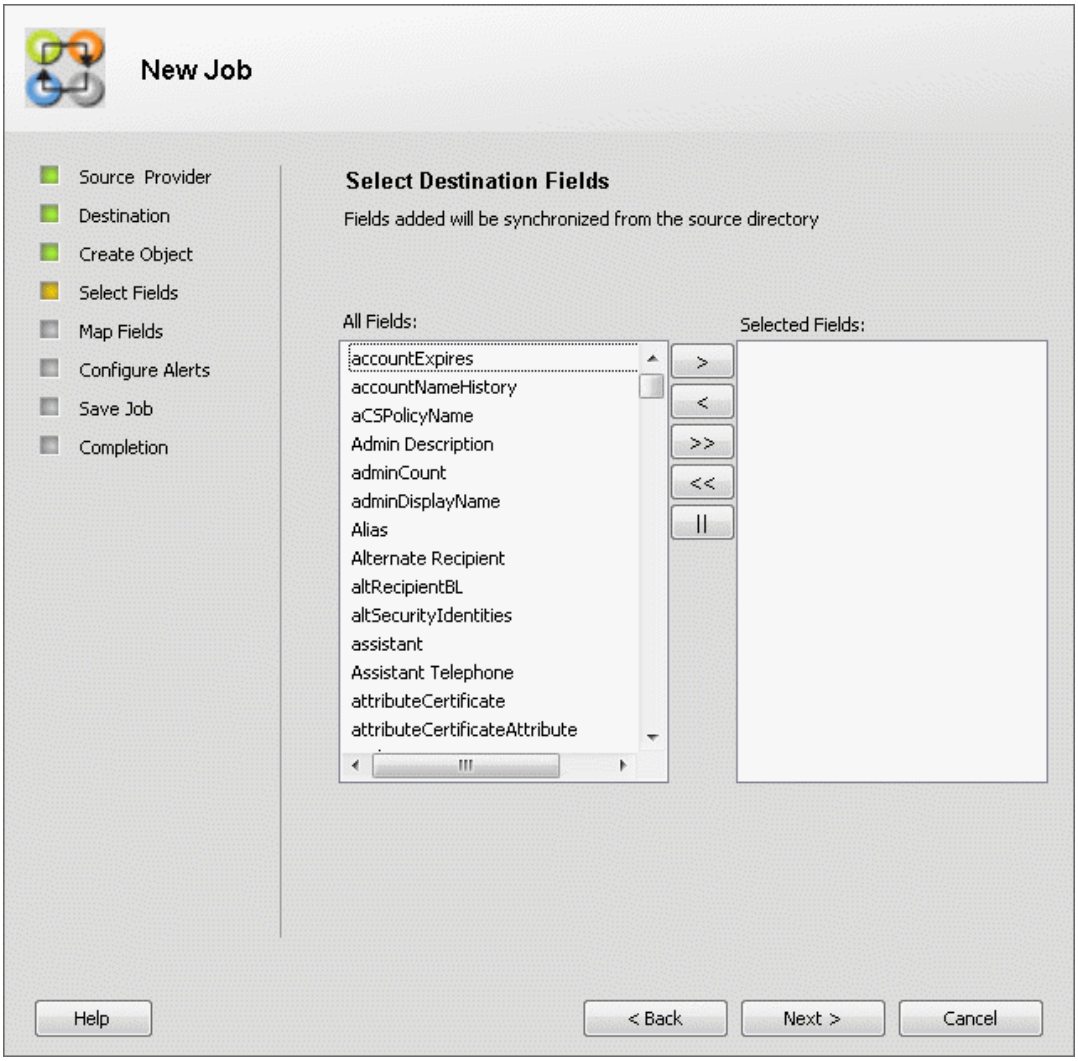


Figure - The Select Destination Fields page.

On this page:

i. From the **All Fields** list, select the names of fields to synchronize.

ii. Click > to move the selected fields to the **Selected Fields** list. By default, Synchronize moves some of the fields to this list by analyzing the fields from the source.

iii. Click **Next**.

7. Use the **Connect Synchronized Fields** page to map the source and destination fields; and to apply any transformations. From the list of fields shown in the **Field Mapping** section, select the source fields for the given destination fields. You may remove any item from the list that you may not require, simply select that item from the list and press DELETE to remove it. From the given list of fields, you will need to specify a **Key** field. A key can be of a single field, or it can be a combination of two or more fields. Whatever the composition, the value of the key fields must be unique.

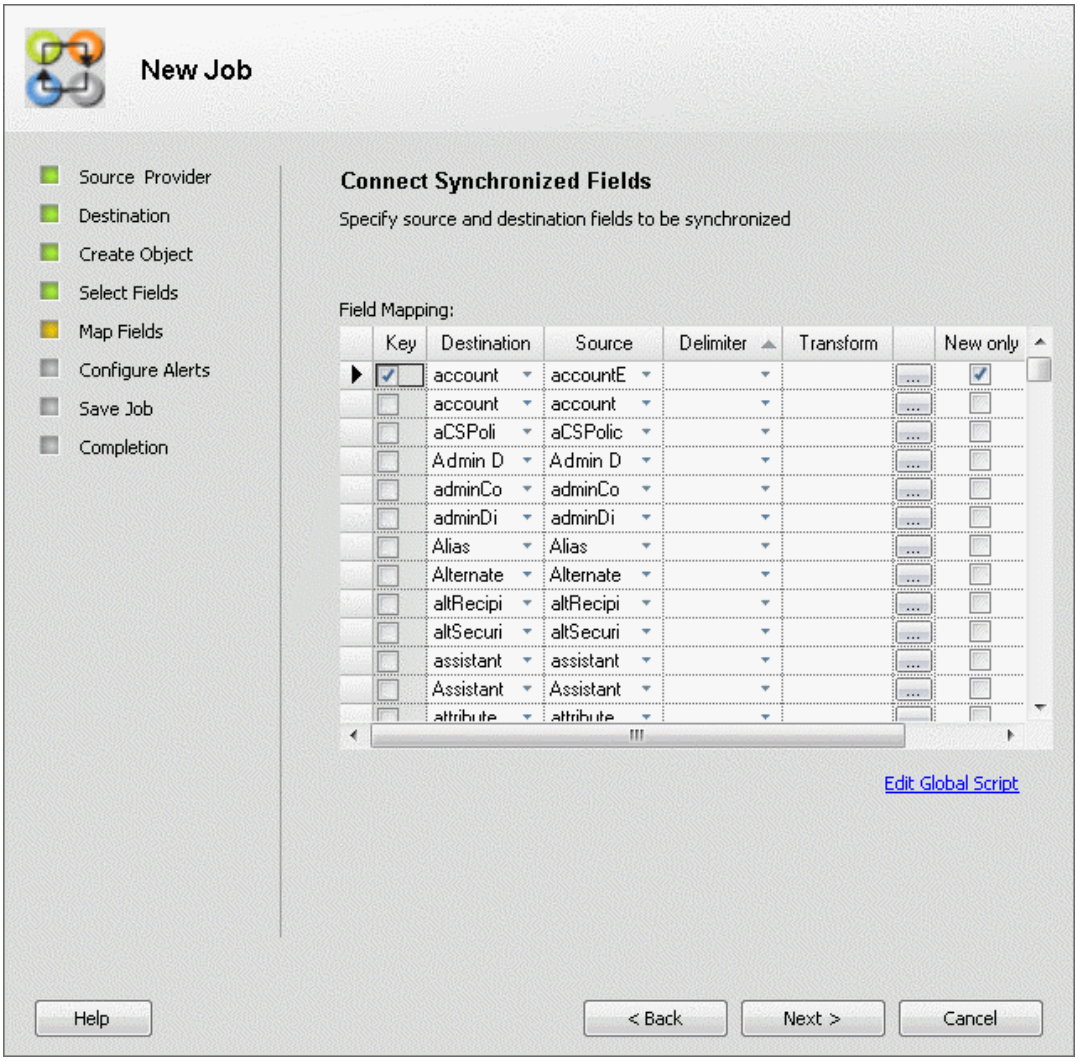


Figure - The Connect Synchronized Fields page.

On this page of the wizard:

i. In the **Key** column, select the check box for the field or fields to mark as unique identifiers. At least one field needs to be defined as a Key.

ii. In the **Source** column, use the list for each destination item to specify the source fields from which to move data into them.

iii. In the **Delimiter** column, specify the character to use for joining or splitting data. Use delimiters for fields containing multiple values, such as multi-value attributes in Microsoft Active Directory. To use delimiters, you must first define them, see **Chapter 18: Synchronize**.

iv. In the **Transform** column, click ... to open the **Transform [*field*]** dialog box and apply a transformation to the field value before it is saved at the destination. Skip this step if you do not want to apply a transformation.

v. In the **New only** column, select the check boxes for fields that should only be updated when creating a new object. Fields, not selected, will be updated always. Fields selected as **Key** will also have this check box selected for them. This is a requirement for a Key field and cannot be undone.

vi. Click **Next** when finished on this page.

8. Use the **Configure Notifications** page to enable your Job to send the results of a Job run in an e-mail. This requires the notification settings to be set for Synchronize. You can configure these settings from the **Configuration** node, clicking **Modify System Configuration** and then clicking **Notifications** tab.

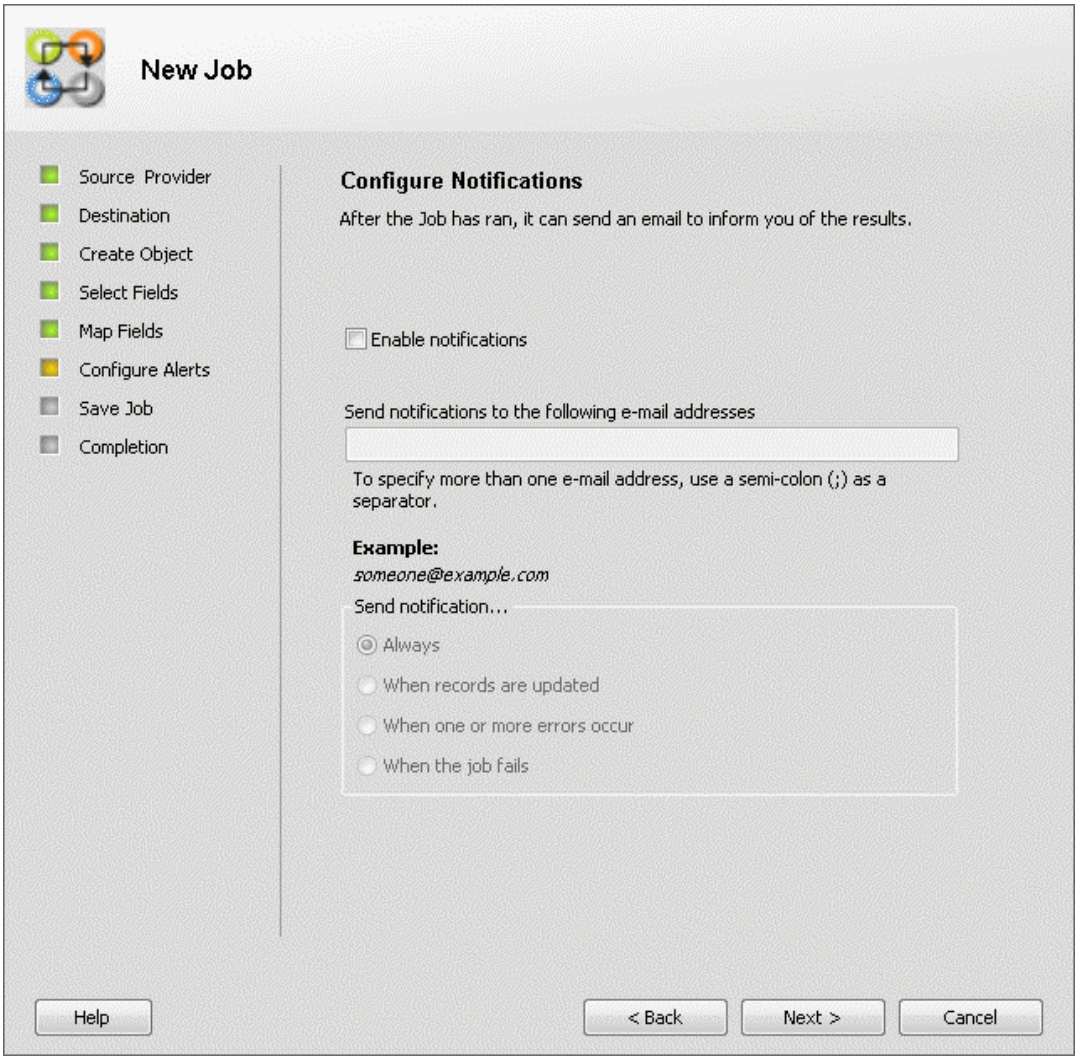


Figure - The Configure Notifications page.

On this page:

i. Select the **Enable Notifications** check box to enable notifications for this Job**.**

ii. In the **Send Notifications to the following email address** box, type the e-mail address on which you want the Job to send notifications to. Use semi-colon (;) as separator for more than one e-mail addresses.

iii. From the **Send notification** list, select the event on which the notification should be sent.

9. Click **Next**.

10. On the **Completing the Synchronize Job Wizard** page, you can see the summary of your new Job based on your selections on the previous pages.

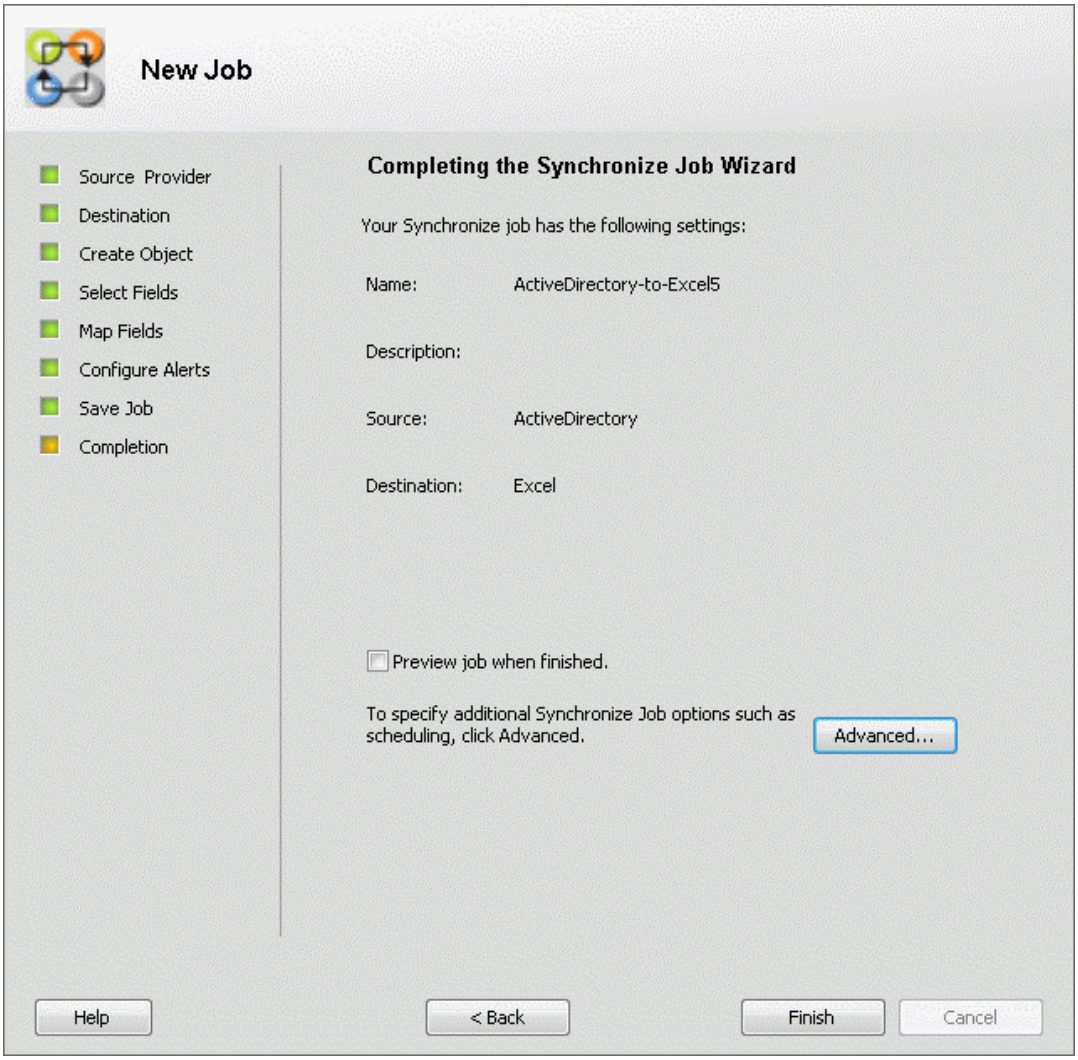


Figure - The Completion page.

On this page:

- Click **Finish** to end the wizard and create the Job.
- Select the **Preview job when finished** check box to have a preview run of the Job after the wizard completes.
- Click **Advanced** to go to advance setting for the Job. See the steps given in the following section if you have selected this option.

Advance Settings for a Job

The advance settings for a Synchronize Job let you:

- Select whether to update all records at the destination or only those that have been modified at source.
- Modify the default LDAP query - this is the query that the job uses to retrieve the data from the source.
- Schedule the Job.

While creating a new Job, the advance settings for the Job can be set by clicking the **Advanced** button on the **Completion** page of the wizard. Clicking **Advanced** displays three additional wizard pages which let you set the three settings mentioned in the list above.

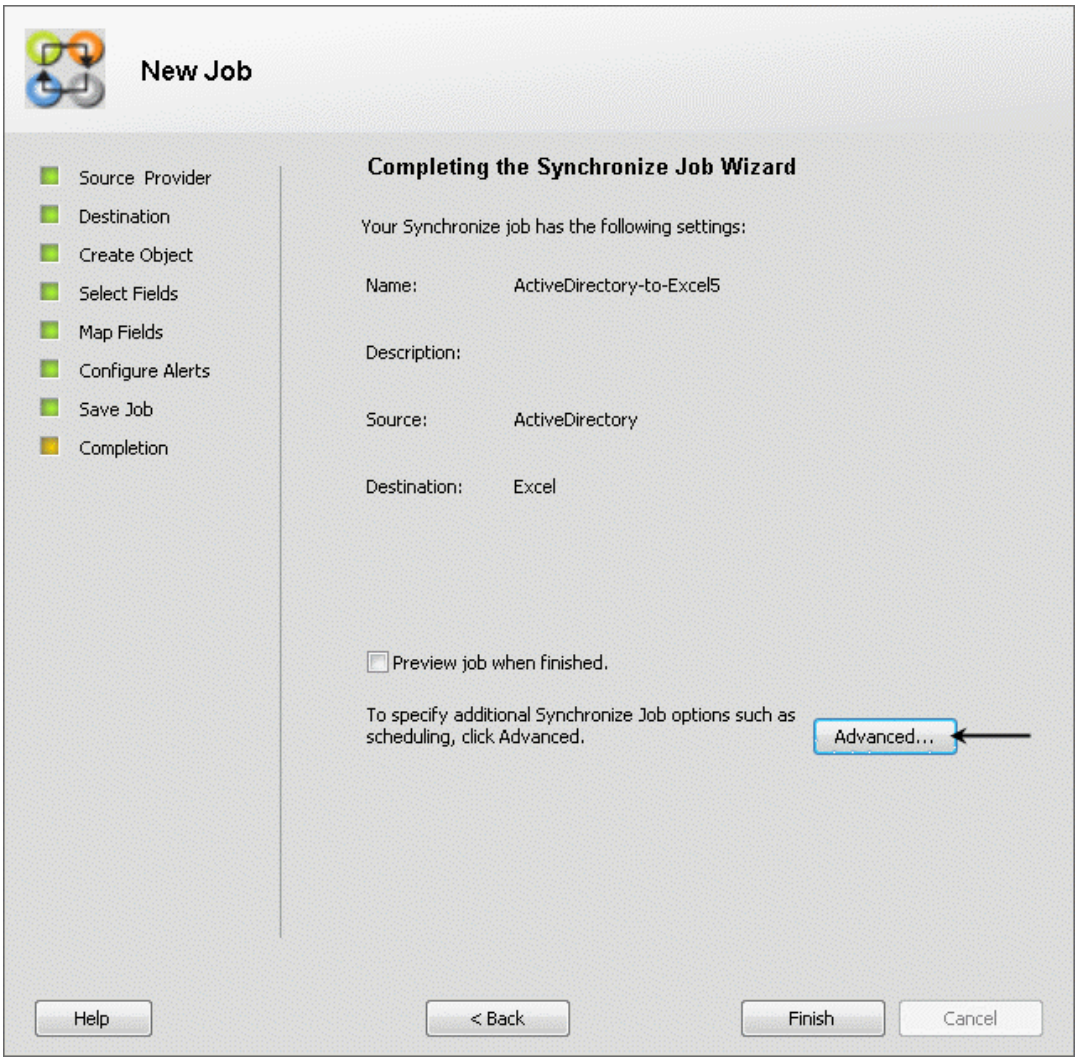


Figure - Highlights the Advanced button on the Completion page.

The following steps list the procedure for the additional wizard pages displayed on clicking the **Advanced** button.

1. On the **Direct Synchronization Settings** page, select whether you want all records to be updated on the destination, or only those that have modified over time. The latter requires you to specify a timestamp field. Using the field specified as timestamp, the Job compares the value of this field for all records at the source and the destination. For any record where a difference is found, it gets updated at the destination.

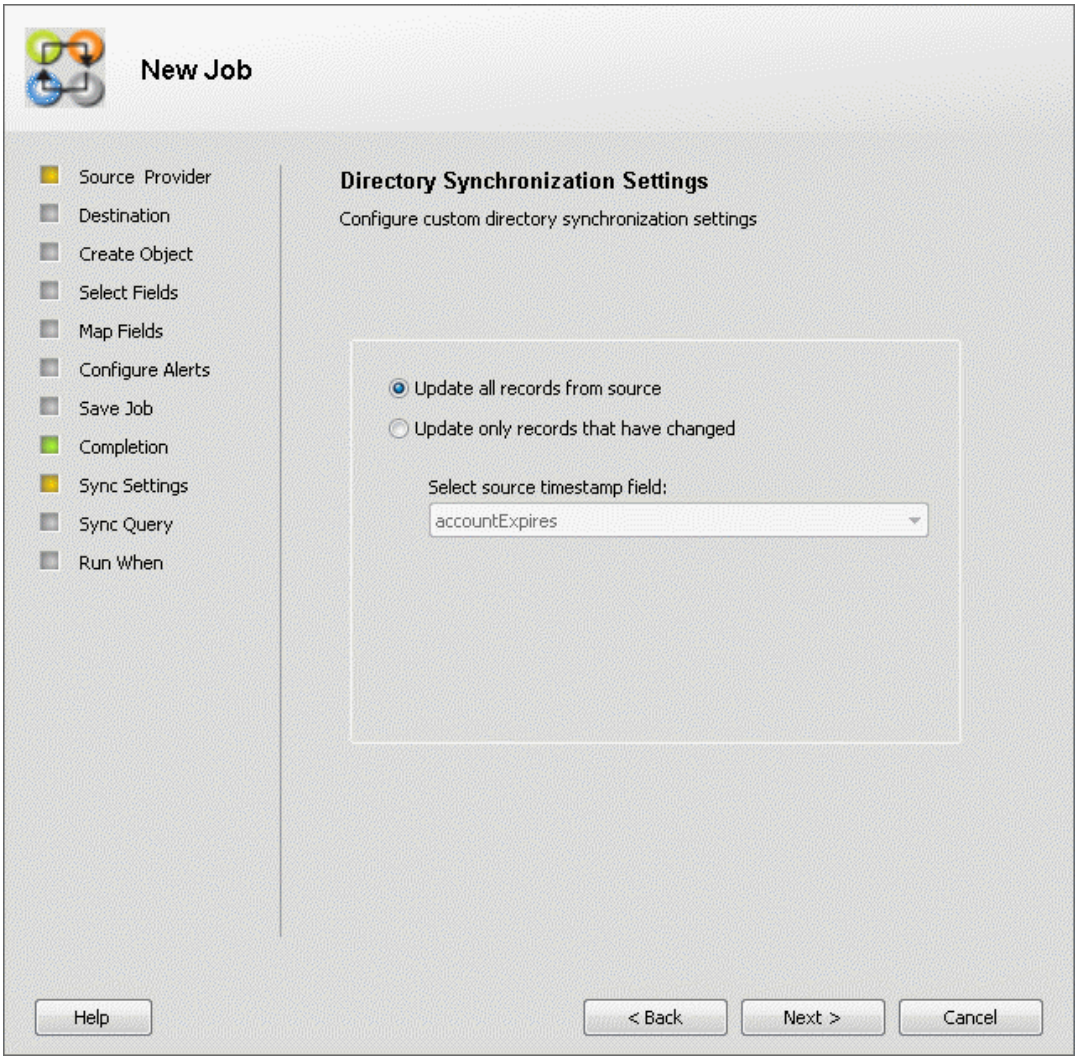


Figure - The Directory Synchronization Settings page.

2. Click **Next**.

3. The **Directory Synchronization Query** page shows the default query statement used for extracting data from the source. Here you can modify the query statement if required.

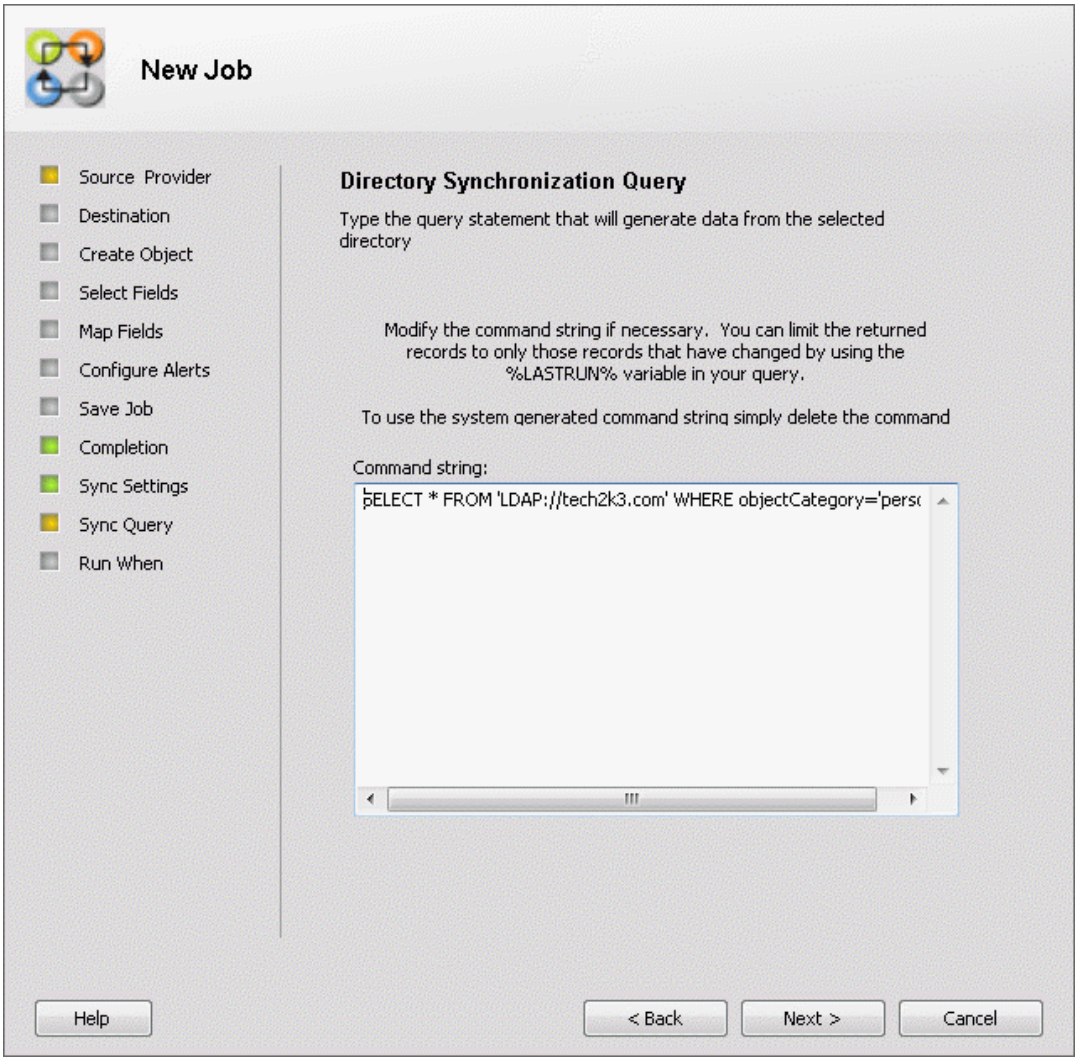

New Job
Source Provider
Destination
Create Object
Select Fields
Map Fields
Configure Alerts
Save Job
Completion
Sync Settings
Sync Query
Run When
Directory Synchronization Query
Type the query statement that will generate data from the selected directory
Modify the command string if necessary. You can limit the returned records to only those records that have changed by using the %LASTRUN% variable in your query.
To use the system generated command string simply delete the command
Command string:
SELECT * FROM 'LDAP://tech2k3.com' WHERE objectCategory='pers
Help
< Back
Next >
Cancel

Figure - Directory Synchronization Query.

4. Click **Next**.
5. Use the **When to Run Job** page to define a schedule for your Job.

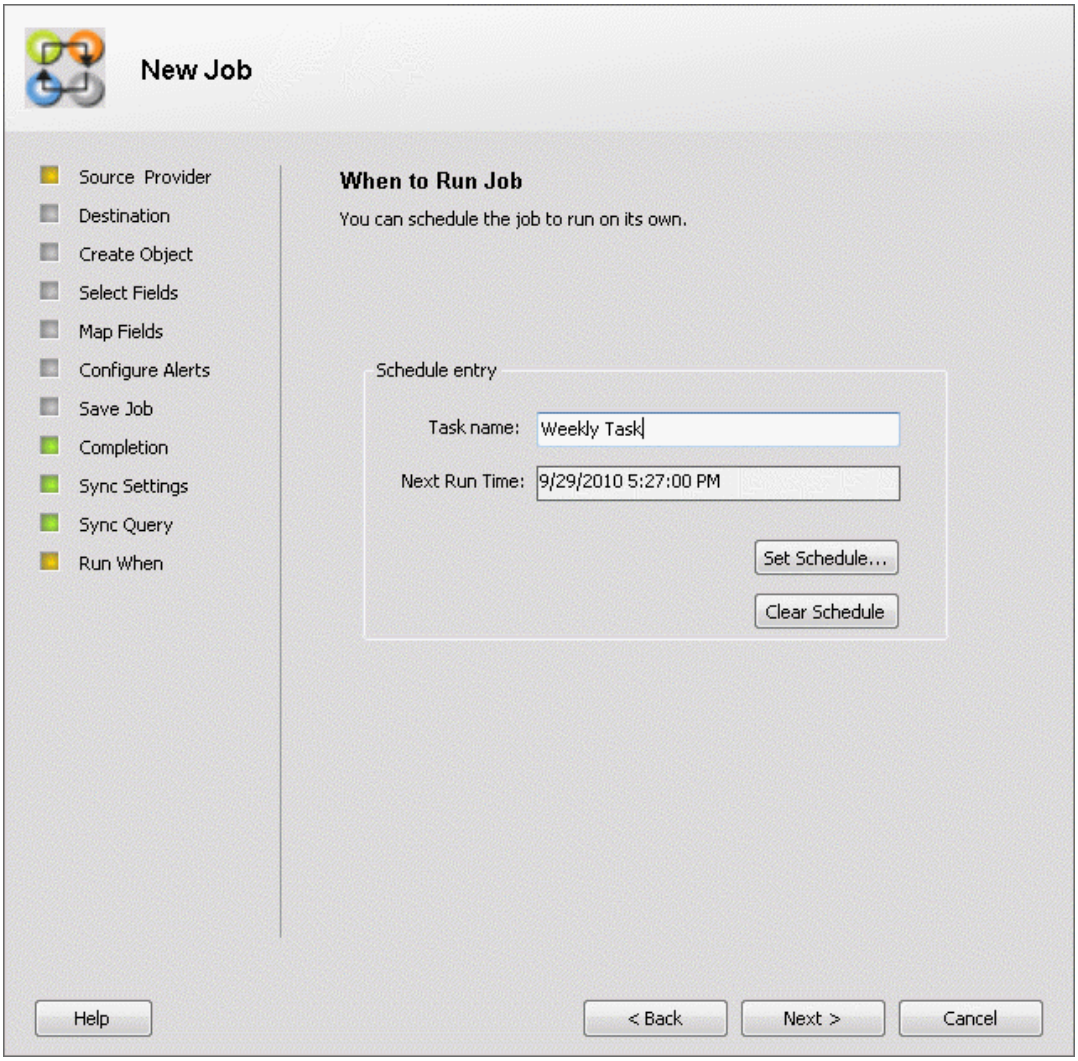


Figure - When to Run Job page.

On this page:

i. In the **Task name** box, type a name for this scheduled task.

ii. Click **Set Schedule** to open the Windows Task Scheduler dialog box and define your schedule.

iii. The next date and time for the next scheduled run will show in the **Next Run Time** box.

iv. Click **Next**.

6. On the Completion page, click **Finish** to end the wizard and create the Job.

Password Policy Validation

When setting static value for the password field, Synchronize validates the specified password with the policy set on the destination Active Directory. This validation will not include the following conditions and hence will not report about them if one or all of them are not being satisfied:

1. **Password History:** This condition prevents a user from setting a previously used password.
2. **Account Name Containment:** This condition prevents a user from setting a password that includes the username as substring of the password.

For conditions, other than those mentioned above, any violation of the destination password policy will require the user to correct the password to proceed.

Previewing Jobs

One of the features of Synchronize is to preview the results of a Job before actually executing it. This saves users from making changes to the actual data at destination side and lets them test if their Job is working as intended or not.

Use the following instructions for previewing a Job:

1. In GroupID Management Console, expand the **Synchronize** node.
2. Click the **All Jobs** node to select it.
3. From the Jobs list, right-click the required Job and click **Preview**.
   This opens the **Preview Job** dialog box which shows the Job run progress.

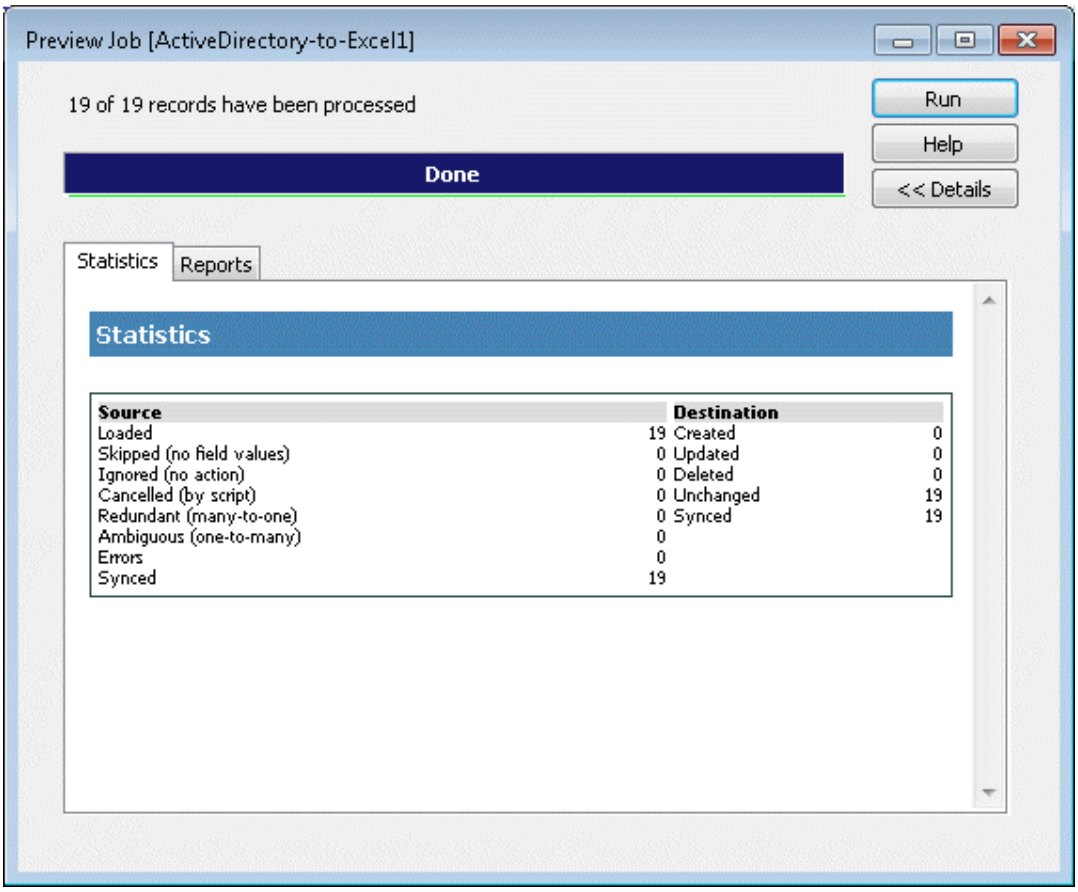


Figure - The Preview Job dialog box

4. When the operation completes, the results can be viewed from the **Statistics** and **Reports** tabs. Note that this run will not make any changes to the actual data sources. To make actual changes to the data sources, you need to Run this Job.

A Job preview provides the user with the following information:

- **Statistics**, shows a summary of the test run providing information on the number of records that are affected at both the source and destination sides.

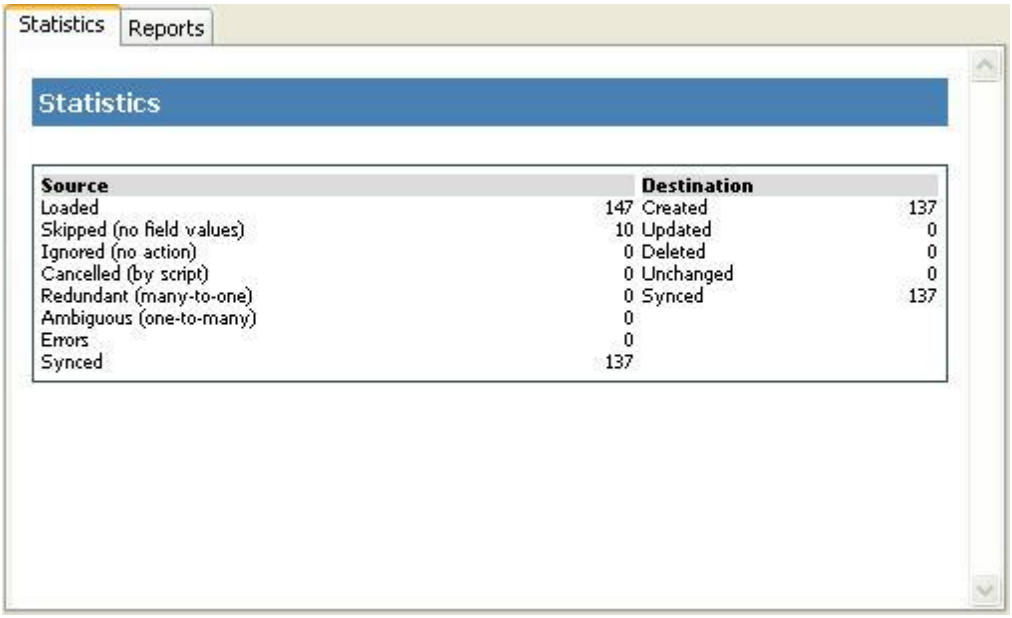


Figure - The Statistics tab of the Job Preview dialog box

- **Reports**, presents a drill down report that shows the records affected. The report provides a breakdown of the records depending on whether they were inserted, updated or deleted as a result of the run.

Figure - The Reports tab of the Job Preview dialog box

Data on the **Reports** tab is displayed in a tabular format. This table consists of three columns: **Error**, **Key** and **Action**.

Column	Description
Error	Shows the error message for a record, if any, encountered during the Job run.
Key	Shows the display name and the value of field(s) marked as **Key**. Key fields are selected on the **Connect Synchronized Fields** page of the wizard when creating or modifying a Job.
Action	Shows the action done against the record, for example: Insert Row, Update Object and similar.

The default grouping of the records shown on this tab is by the **Action** column. You can change this by dragging other columns into or out of the grouping area - this area is highlighted in the figure below.

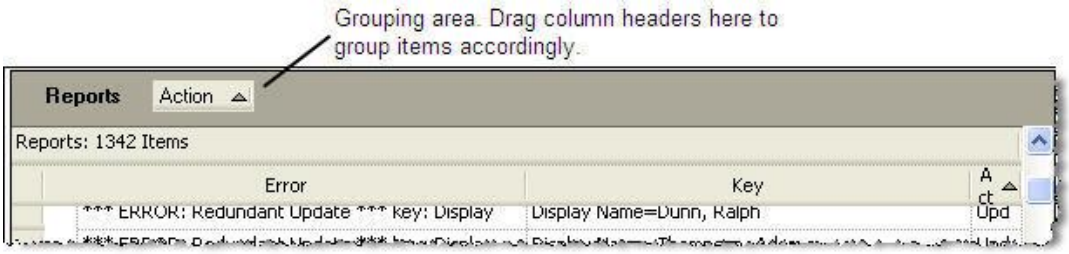


Figure - Highlights the grouping area on the Reports tab

Running Jobs

Running a Job carries out the data transfer operation. It makes changes to the data at the destination as per the settings of the Job.

To run a Job:

1. Expand the **Synchronize** node and click **All Jobs**.
2. From the list, right-click the required Job and click **Run**.
   This opens the **Run Job** dialog box showing the progress of the Job as it runs.
3. Once the Job run completes, click **Details** to expand the **Run Job** dialog box and view details which include statistics, reports and logs for it.

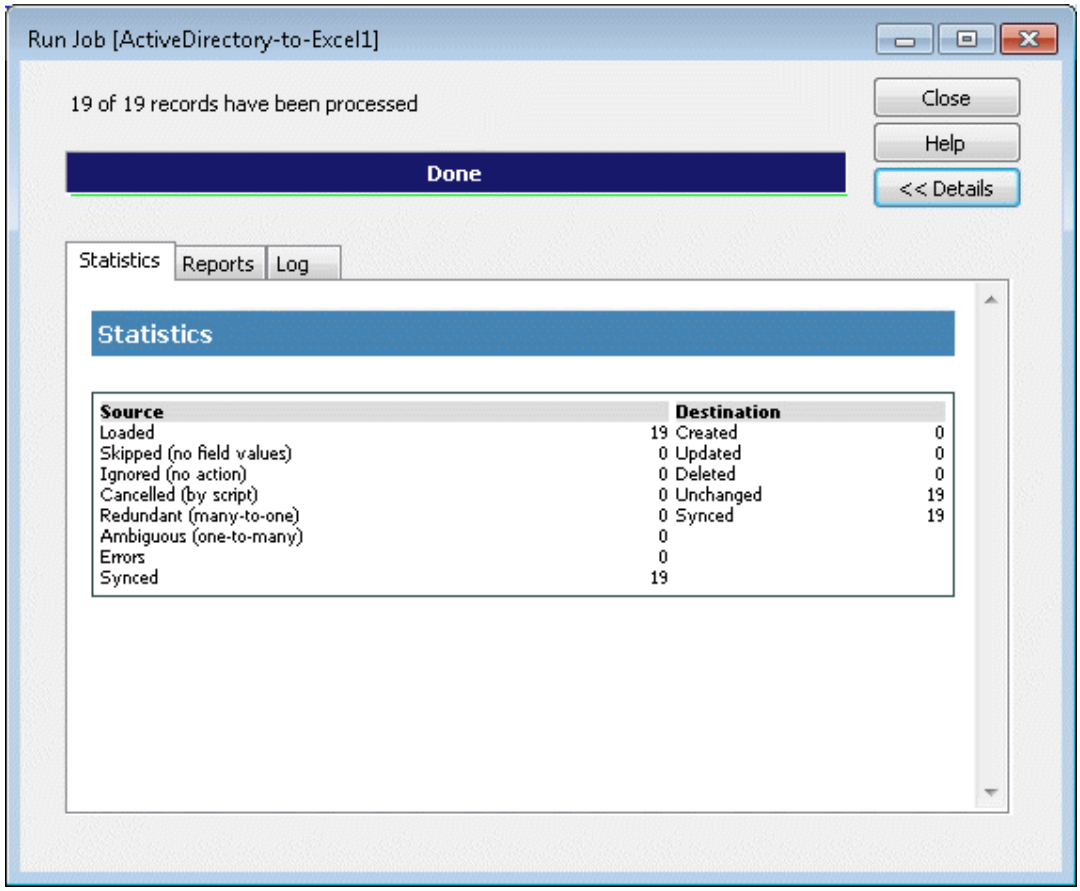


Figure - The Run Job dialog box.

The details included in the **Run Job** dialog box are similar to those in the **Preview Job** dialog box with one additional tab which shows the Job log. More information on logging is covered in the topic **Logging Job Run Activities** later in this chapter.

Results of every Job run are saved to a specific location on your computer as individual files. These files are in XML format and can be viewed by opening them in any XML or text editor program, like Windows Notepad. Except for the results of the last run, the results of previous Job runs cannot be viewed through the **Run Job** dialog box or any other Synchronize user interface.

To view the results of your last Job run, right-click the Job in the Jobs list, and then click **Review Last Job Run**.

To view the result files for history Job runs, see the topic **Job Files**.

Synchronize Command-line Utility

The command-line utility for Synchronize is designed to facilitate running synchronization jobs using the Windows command prompt. When you create a job, a configuration file is generated containing all settings of the job and is stored in a particular directory on your machine. Synchronize command-line utility requires this configuration file to run the job. For information about the location of the job configuration file, see **Job Files** later in this chapter.

This utility is available in the installation directory for GroupID by the name **Imanami.GroupID.Synchronize.exe**.

To run a synchronization job through command-line utility:

1. On the command prompt, move to the installation directory for GroupID. By default, GroupID is installed to the location: **C:\Program Files\Imanami\GroupID**.

2. Type the following command:

```
Imanami.GroupID.Synchronize "path of the configuration file\configuration file name.dtmconfig"
```

3. Press **Enter** to run the command. This will execute the job and show the job progress and statistics as it runs. If some errors occur while running the job, the utility displays them as well on the command prompt.

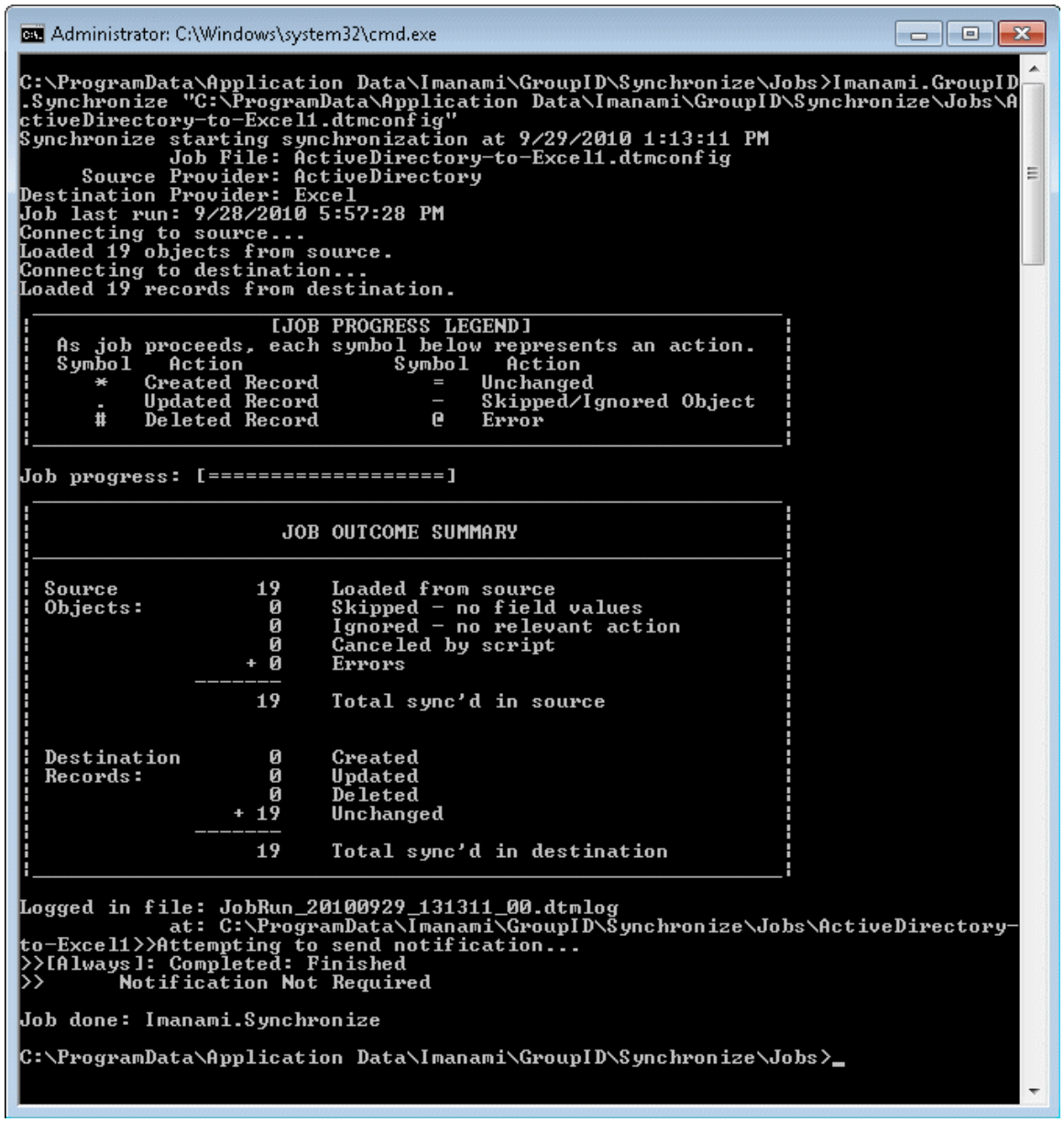

Administrator: C:\Windows\system32\cmd.exe
C:\ProgramData\Application Data\Imanami\GroupID\Synchronize\Jobs>Imanami.GroupID.Synchronize "C:\ProgramData\Application Data\Imanami\GroupID\Synchronize\Jobs\ActiveDirectory-to-Excel1.dtmconfig"
Synchronize starting synchronization at 9/29/2010 1:13:11 PM
Job File: ActiveDirectory-to-Excel1.dtmconfig
Source Provider: ActiveDirectory
Destination Provider: Excel
Job last run: 9/28/2010 5:57:28 PM
Connecting to source...
Loaded 19 objects from source.
Connecting to destination...
Loaded 19 records from destination.
[JOB PROGRESS LEGEND]
As job proceeds, each symbol below represents an action.
Symbol Action Symbol Action
* Created Record = Unchanged
. Updated Record - Skipped/Ignored Object
Deleted Record @ Error
Job progress: [====================]
JOB OUTCOME SUMMARY
Source Objects: 19 Loaded from source
0 Skipped - no field values
0 Ignored - no relevant action
0 Canceled by script
+ 0 Errors
19 Total sync'd in source
Destination Records: 0 Created
0 Updated
0 Deleted
+ 19 Unchanged
19 Total sync'd in destination
Logged in file: JobRun_20100929_131311_00.dtmlog
at: C:\ProgramData\Imanami\GroupID\Synchronize\Jobs\ActiveDirectory-to-Excel1>>Attempting to send notification...
>>[Always]: Completed: Finished
>> Notification Not Required
Job done: Imanami.Synchronize
C:\ProgramData\Application Data\Imanami\GroupID\Synchronize\Jobs>

Figure - the command prompt showing the job progress and statistics

Scheduling Jobs

A Job can be scheduled when you are creating it, or later on when required. To learn how to schedule a Job when creating it, refer to the topic, **Creating a Job**.

To schedule a previously unscheduled Job:

1. Expand the **Synchronize** node and click **All Jobs**.
2. From the list, right-click the required Job and click **Schedule**.
   This opens the When to Run Job page.

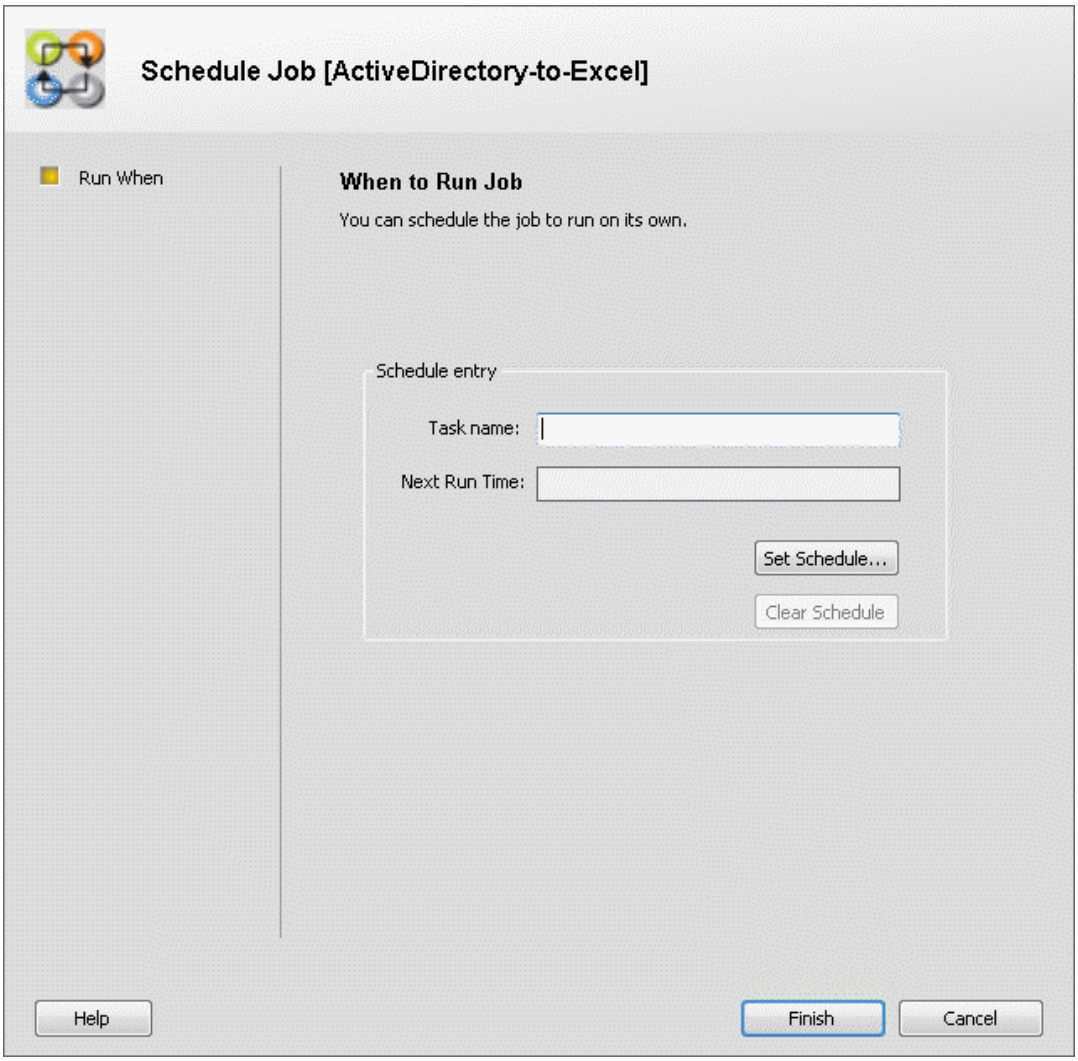


Figure - Schedule Job page.

3. On the **When to Run Job** page:
   i. In the **Task name** box, type a name for this task.
   ii. Click **Set Schedule**.
   This opens the **New Task** dialog box.

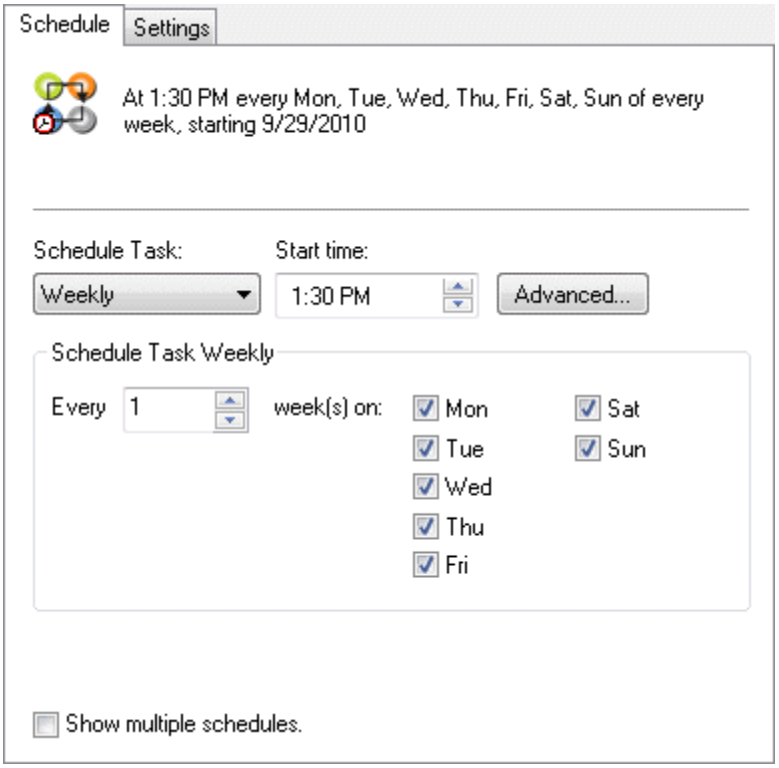


Figure - The Schedule tab.

iii. On the **Schedule** tab, select the frequency for this task from the **Schedule Task** list. The required settings for the selected frequency will show in the **Schedule Task** section below this list.

iv. In the **Start time** box, type or select the time of the day when to run the Job.

v. From the **Schedule Task** section, set the fields as per your requirements.

vi. Click **OK** to save your new scheduled task.

4. Click **Finish** to save your new schedule for the selected Job.

Creating Multiple Schedules for a Job

If you would like to create multiple schedules for a Job, select the **Show multiple schedules** check box on the **Schedule** tab.

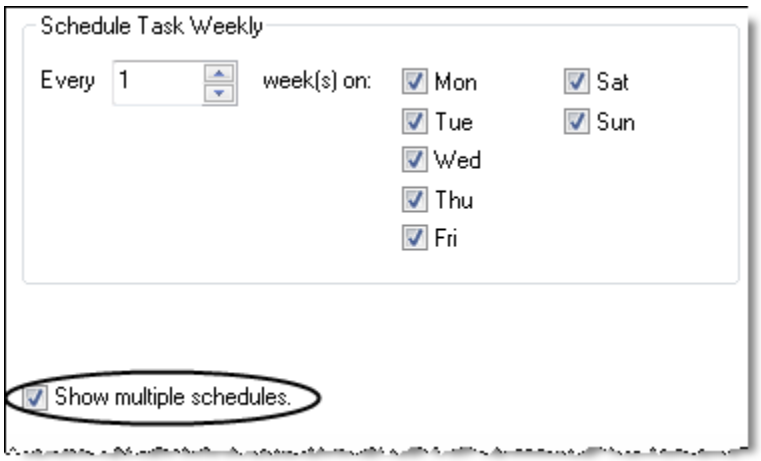


Figure - Highlights the Show multiple schedules check box.

This changes the top section of the tab to display additional fields for handling multiple schedules, see figure below. The selected schedule in the list is the active schedule.

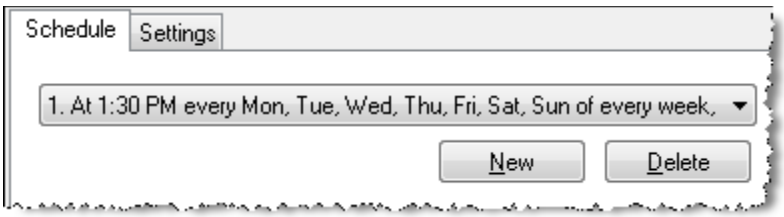


Figure - Top section of Schedule tab changes to display a list with New and Delete buttons to create and remove additional schedules.

Synchronize uses Microsoft Windows APIs task scheduling. For more information on scheduling and to learn about its advance features, refer to Windows Help.

Job Files

Synchronize maintains three types of files for every Job. These files include the:

1. Job configuration file
2. Job report file
3. Job log file

The location where these files are stored depends upon the version of Windows installed on your computer. You can find out the location of this directory using the Windows **%ALLUSERSPROFILE%** environment variable. On the Windows **Run** dialog box, type the following command:

```
%ALLUSERSPROFILE%\Application data\Imanami\GroupID\Synchronize\Jobs
```

The Job configuration file

The Job configuration file is the main file containing all settings for a Job. This file is created when a new Job is defined. This file is saved with the **.dtmconfig** extension in the **Jobs** directory at the location specified above. See **Creating a Job** to learn more about creating Synchronize Jobs.

The report file

The report file is generated when a Job is run. This file is saved with the **.dtmreport** extension. This file contains the records and objects inserted, updated, removed or exchanged on the source and destination. The data from this file is also displayed in the **Reports** tab of the **Job Run** dialog box. See **Running Jobs** to learn more about the **Run Job** dialog box.

Synchronize creates a new report file every time a Job is run and archives it. Unlike the Job configuration file, the report files are saved in a sub-directory created on the name of the Job itself under the **Jobs** directory.

The log file

The log file is also generated along with the report file during a Job run and displayed on the **Log** tab of the **Run Job** dialog box. This file is also saved in the same location as the report file with the **.dtmlog** extension. Data written to the log file depends on the **Logging** setting set for your Synchronize. This setting can be set from the **Configurations** section.

Synchronize creates a new log file every time a Job is run and archives it.

Logging Job Run Activities

There are many actions taking place in the background when a Job is run. These actions are logged and displayed on the **Log** tab of the **Run Job** dialog box.

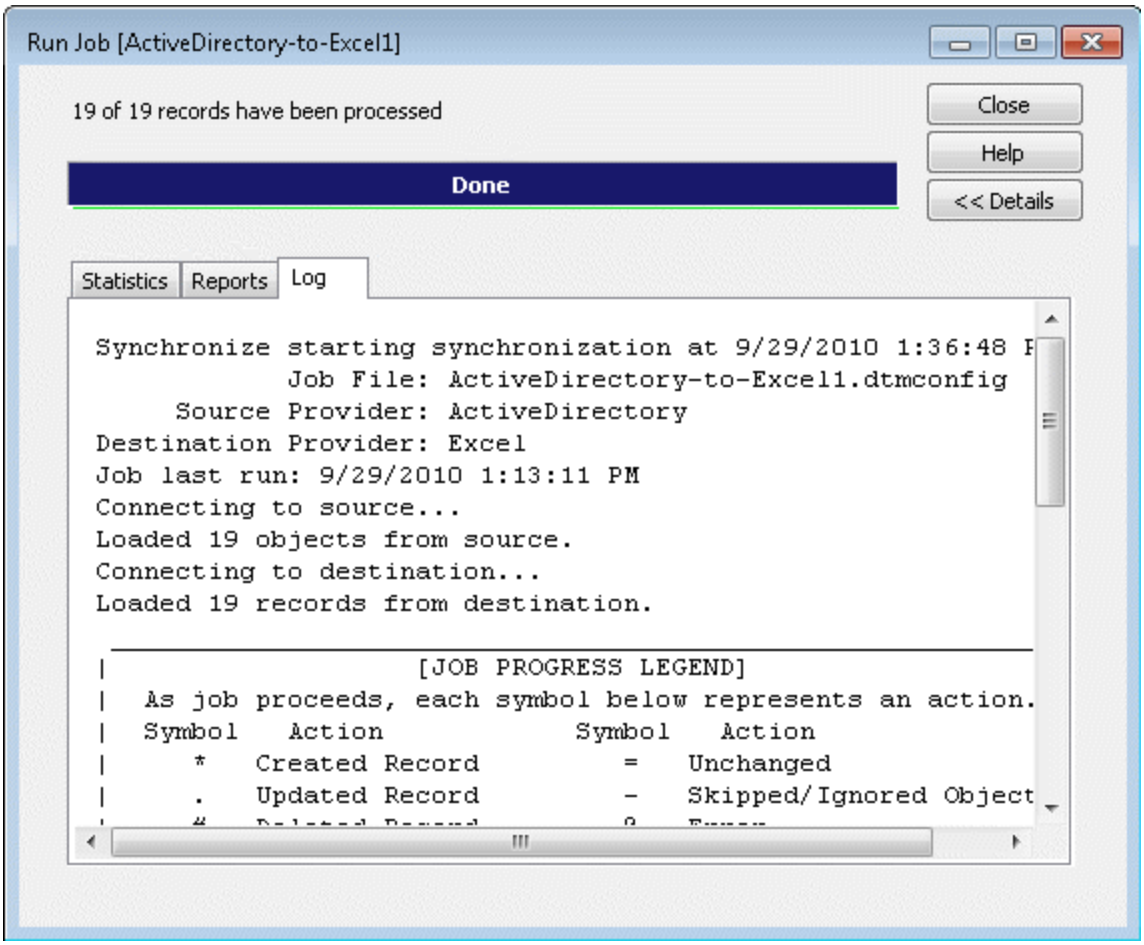


Figure - Shows the Log tab on the Job Run dialog box.

The information contained in a log file depends on the logging level set in the global configurations of GroupID. Refer to the **Log Settings** topic in **Part : GroupID Configurations**, to learn more about logging.

Logs for every Job run are archived and stored on disk. See the topic **Job Files** to learn more.

Chapter 16: Transformations

This chapter introduces you to transformations. It introduces you to the types of transformations available in Synchronize and explains them in detail.

Static Transformation, introduces you to Static transformation and its use.

Join Transformation, introduces you to Join transformation and its use.

SubString Transformation, introduces you to SubString and its use.

Left Transformation, introduces you to the Left transformation and its use.

Script Transformation, introduces you to the Static transformation and its use.

Static Transformation

A static transformation copies static text to the destination field for all records irrespective of their value at the source. This transformation is useful if you want to insert a specific value into a destination field irrespective of what value exists for it at the source end.

> If you plan to use this transformation for setting passwords for user accounts on an Active Directory destination, please also read the topic **Password Policy Validation** in this chapter.

By selecting, **Static - assign a static value** from the **Transform** dialog box, you will see the required input fields for the transformation. For this transformation, you need to type the text in the **Static text** box that you want to be copied for this field at destination.

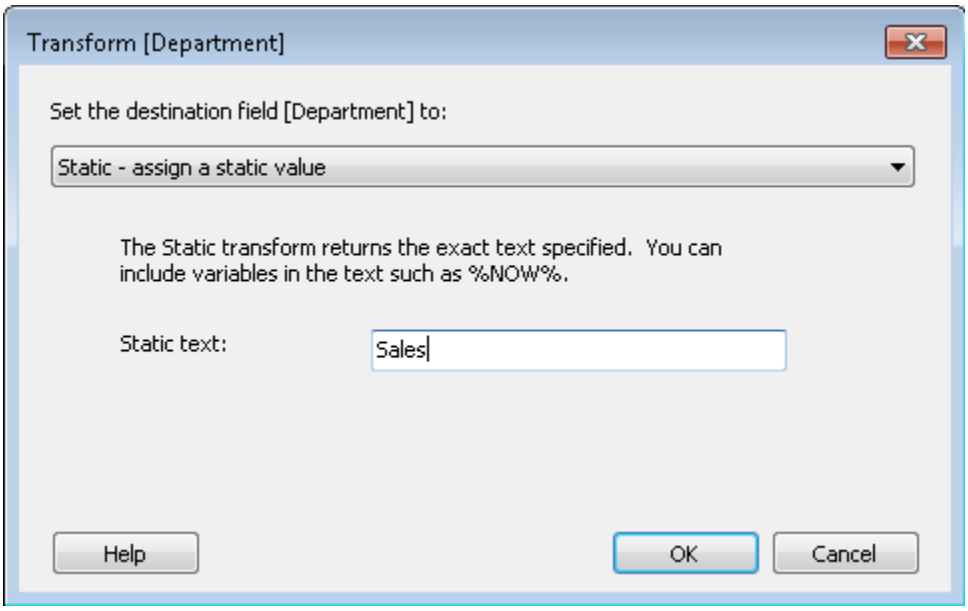

Transform [Department]
Set the destination field [Department] to:
Static - assign a static value
The Static transform returns the exact text specified. You can include variables in the text such as %NOW%.
Static text:
Sales
Help
OK
Cancel

Figure - Transform dialog box showing the required fields for Static transformation.

In addition to static text, you can also specify Windows environment variables. While transferring the data during a Job run, the Job obtains the current value of the variable and saves it to field on the destination side.

Example
If **Static text** is set to **%COMPUTERNAME%**, running the Job will save the host computer's name in the target field.

> Environment variables may vary for different Windows releases and editions. Before using environment variables, determine that they are supported by the Windows installed on your host machine.

Join Transformation

This transformation joins values from two different fields before saving them as one to the target field. For example, you may have two fields **FirstName** and **LastName** at the source and a field **Name** at the destination. By applying the Join transformation, you can join the values for the two source fields and have them saved as a single value in a destination field called **Name**.

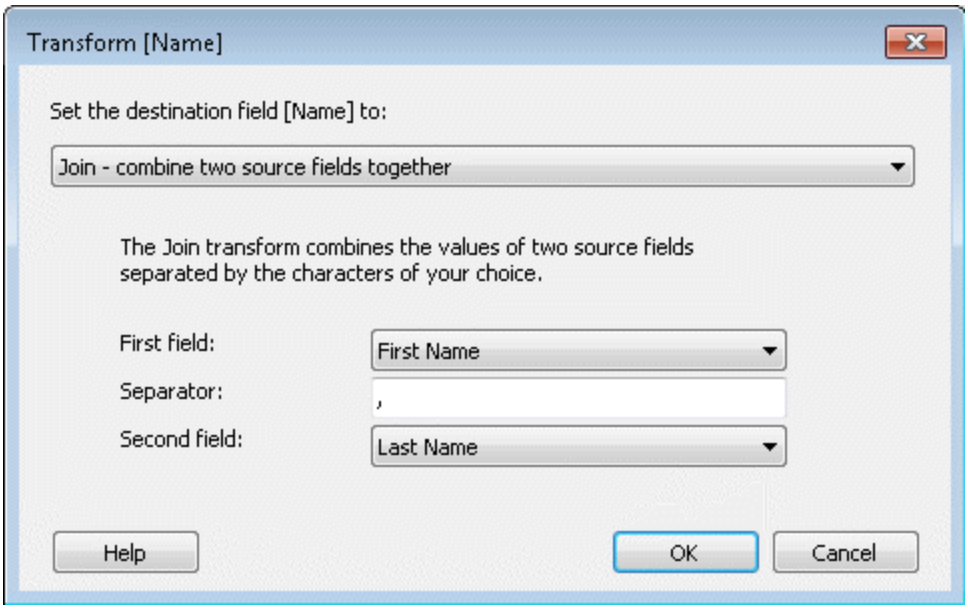


Figure - Transform dialog box showing the required fields for Join transformation.

A Join transformation requires three input parameters. These are as given in the following table:

	Parameter	Description
1	First field	Select from this list the first source field.
2	Separator	Specify here the character to use as separator between the values of the two fields. You can use specify more than one characters separators.
3	Second field	Select from this list the second source field.

Substring Transformation

The Substring extracts a set of characters from the source value and saves it to the destination field. The range of characters to extract from the source value is specified by the user. Substring transformation is useful in cases where the set of characters to extract are from within a value that has a fixed number of characters or digits. The use of this transformation can become tricky if the number of characters or digits in values of the source field may vary.

The Substring transformation requires three inputs. These are as given in the table below:

	Parameter	Description
1	Source field	Select from this list the source field from which to get the value.
2	Start at	Specify here the index number of the character to set as the starting point. The character at this position will not be included in the result itself.
3	Length	This represents the count of characters to extract from the starting

	Parameter	Description
		point.

Example
Telephone numbers are usually written with country and city codes. You may have a destination field where you may only require the city code to be copied excluding the number itself and the country code preceding it.

Consider the number, +92-42-5787711. Where:

Country Code	City Code	Telephone
92	42	5787711

To extract the city code, you would set the parameters for this transformation as shown in the following figure:

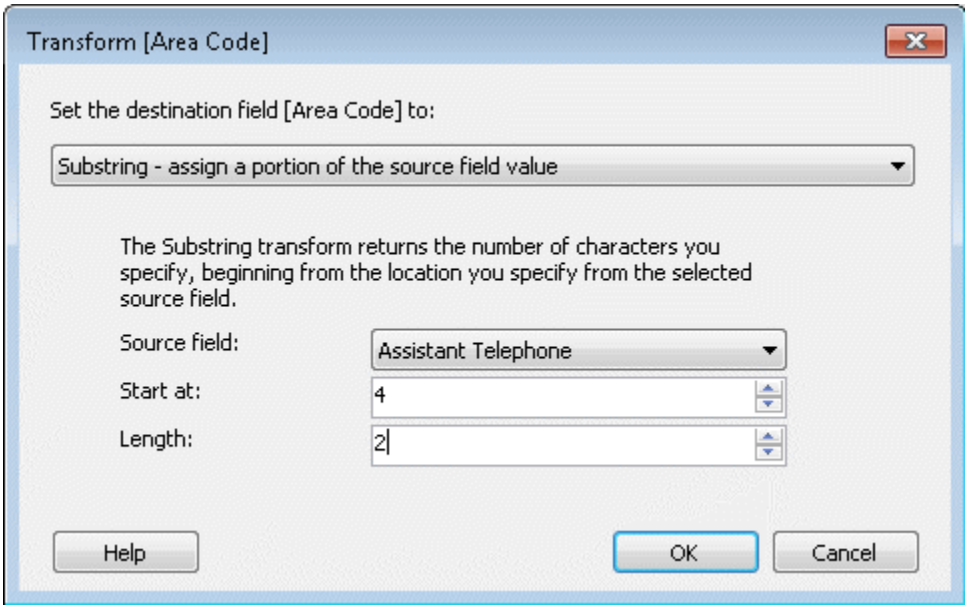

Transform [Area Code]
Set the destination field [Area Code] to:
Substring - assign a portion of the source field value
The Substring transform returns the number of characters you specify, beginning from the location you specify from the selected source field.
Source field:
Assistant Telephone
Start at:
4
Length:
2
Help
OK
Cancel

Figure - Transform dialog box showing the required fields for Join transformation.

When executed, this would extract **42** from the number and save it to the destination field.

Left Transformation

This transformation extracts the specified number of characters from a value starting from its left-side. The Left transformation requires two parameters to be set. These are as given in the table below.

	Parameter	Description
1	Source field	Select from this list the source field from which to get the value.

	Parameter	Description
2	Number of characters	Specify here the number of character to extract starting from the left.

Example
Your requirement is to set the first three characters of a user's logon name as their initials. You can easily achieve this using the Left transformation using the settings as shown in the following figure.

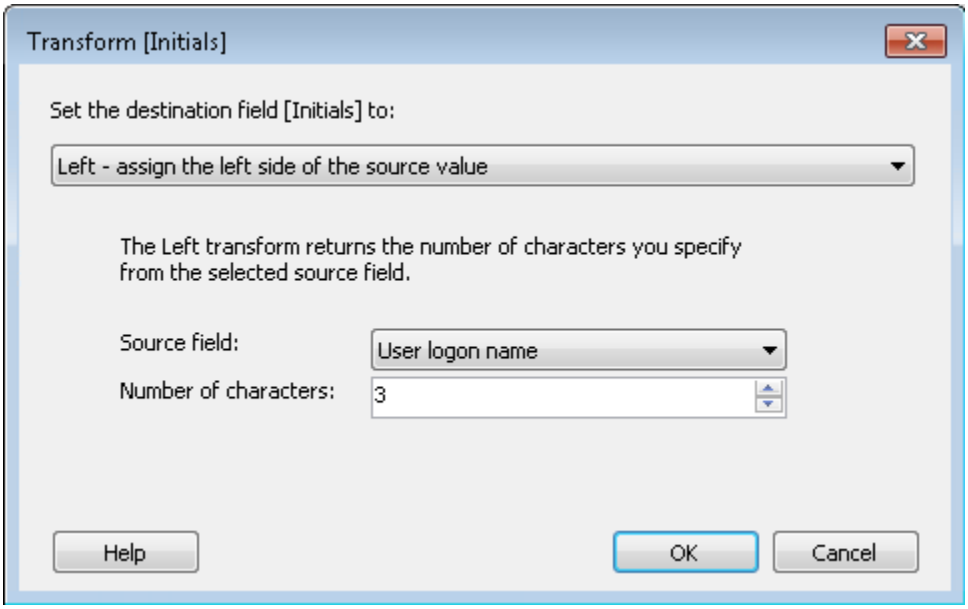

Transform [Initials]
Set the destination field [Initials] to:
Left - assign the left side of the source value
The Left transform returns the number of characters you specify from the selected source field.
Source field:
User logon name
Number of characters:
3
Help
OK
Cancel

Figure - Transform dialog box showing the required fields for Left transformation.

Script Transformation

The script transformation is for performing complex data transformations which will usually include a custom logic that you want to apply on the data being transferred. This transformation is meant for advance users and requires programming in Visual Basic .NET.

Script transformation can be selected using the **Script - write a Visual Basic .NET script to assign a value programmatically** option. Selecting this option shows you the default script which is based on current mapping of the selected field. To change this script and write your own custom logic for data transformation, click **Edit Script** to launch the Script Editor. For more information, refer to the topic **The Script Editor** in **Chapter 17: Scripting**.

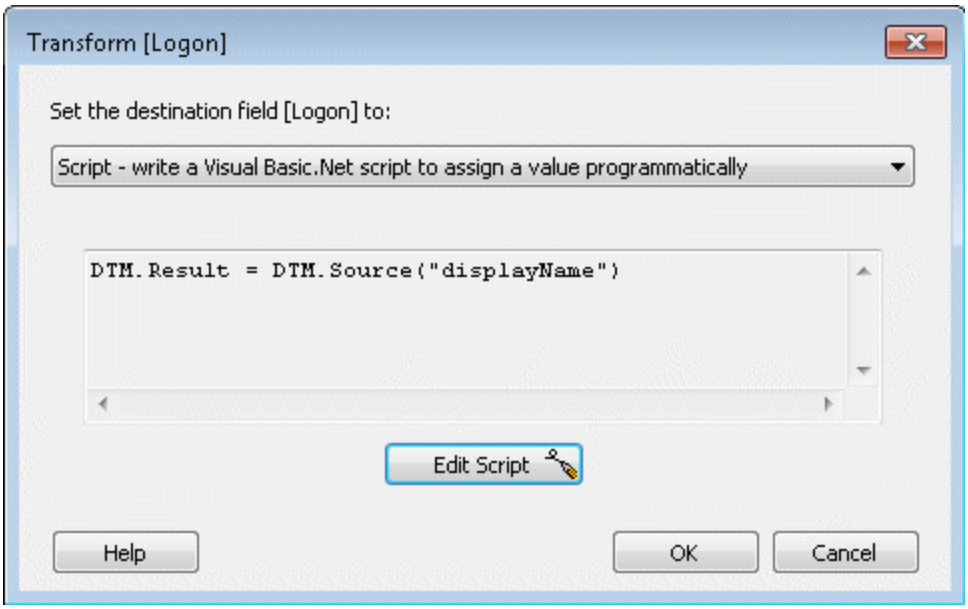


Figure - Transform dialog box showing the required fields for Left transformation.

Chapter 17: Scripting

This chapter provides comprehensive information about scripting in Synchronize. It introduces you with different scripting environments, some scripting restrictions, important aspects of script compilation and so on. The chapter is divided into following sections:

The Script Editor, familiarizes you with the Script Editor and explains how you can use it to write your custom scripts.

Scripting, introduces you to the environments that Synchronize supports for scripting.

DTM, provides information about DTM objects and explains how you can use them in scripting.

The Global Script Editor, familiarizes you with the interface of the Global Script Editor.

VB Options Set by Synchronize, explains Option statements set by Synchronize.

Scripting, describes restrictions that apply while scripting in Synchronize.

.Net Assembly References, describes system assembly references that Synchronize establishes before compiling your scripts.

.Net Namespaces, describes namespaces that Synchronize imports when compiling your scripts.

The Script Editor

The **Script Editor** is a utility for writing Visual Basic .NET script. This can be launched from two locations on the Job wizard:

1. From the **Create Object** page of the Create and Edit Job wizards, when the destination data source is a directory service, by following the steps below:
    i. Select **Create the Object in the destination**.
    ii. Select **Create Objects in a container specified in script**.
    iii. Click **Edit Script**.
2. From the **Transform** dialog box, when the **Script** transformation is selected and **Edit Script** is clicked.

The script editor lets you write script, save it, open existing script files and test your script. The script files are saved with the .vb extension.

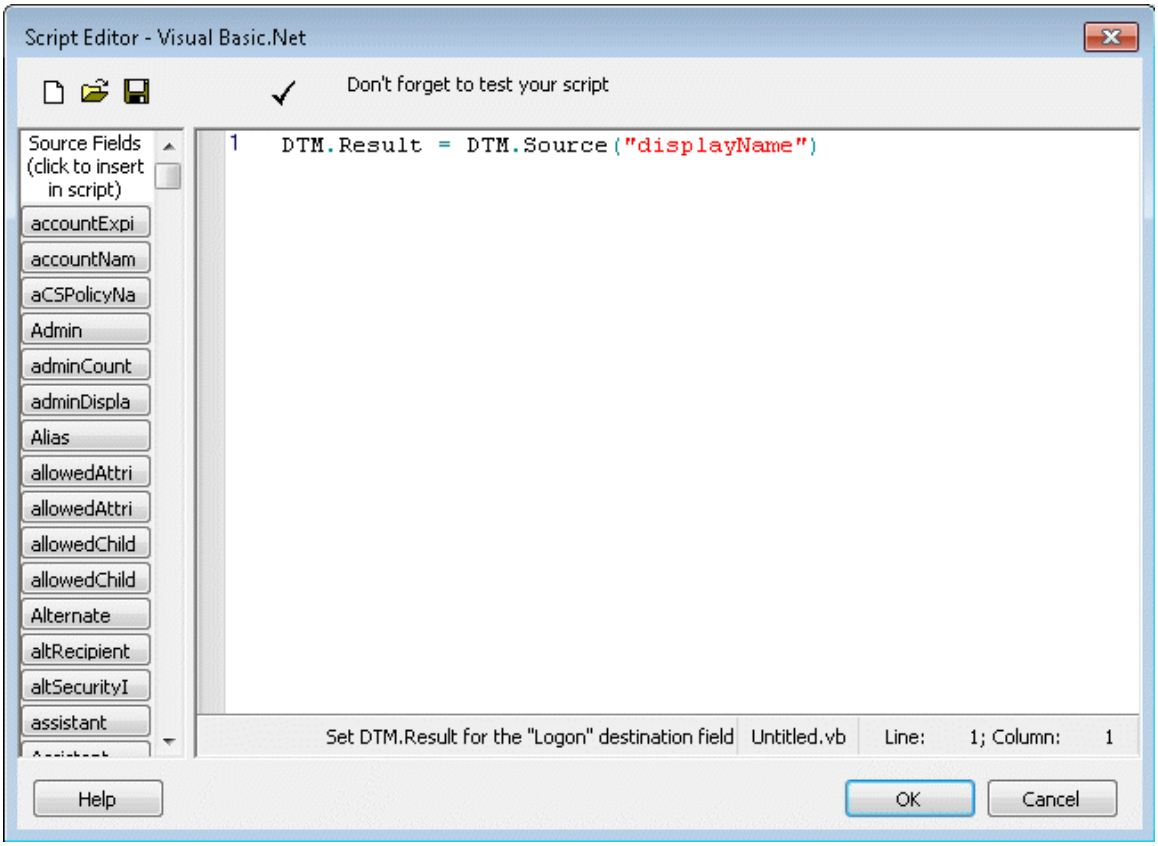


Figure - The Script Editor

The common file commands, new, open, save and test are given in the toolbar of the editor. The left pane shows the list of directory fields that can be used in the script with the **DTM** object. For example:

```
DTM.Source("displayName")
```

To learn more about the DTM object, see the section **DTM Object**.

Testing your script

To test your code, click once you have written it. This opens the **Script Test** dialog box. The Script Tester lets you test your script by using test data. The Script Tester generates input fields in the **Source Fields** section based on the source fields that you specified in your code. It then identifies the destination field and shows the resultant value in the **Destination Field** section.

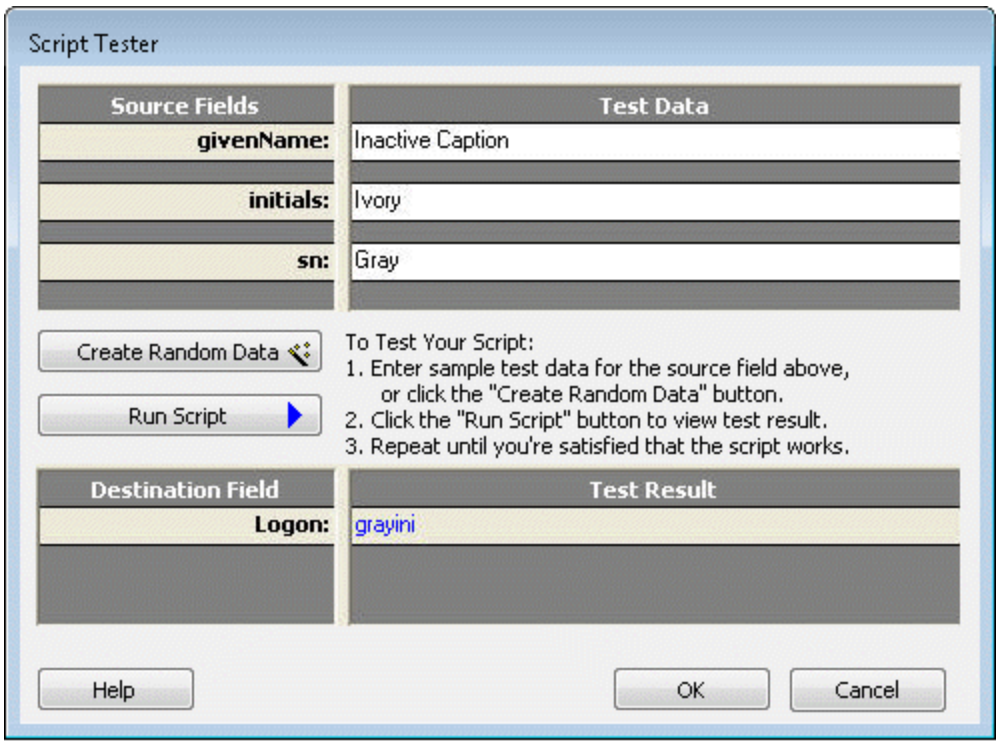


Figure - The Script Tester

To test the script, enter values for the source fields, and then click **Run Script**. This will show the required result in **Test Result**.

You can also test against random test data generated by the Script Tester itself. For this, click the **Create Random Data** button.

Click **OK** when you are done testing your script to close Script Tester. It is important to know that Script Editor will not allow you to save your transformation script until you have run the Script Tester and tested your code.

Script Transformation Example

The following script generates a logon name based on the following format: L5F1I1, where;

L5 = First five characters of the last name
F1 = first character of the first name
I1 = first character of the user's initial

Example: For "Steven T. Segal", the logon name generated by the script will be SegalST.

```
Dim sResult As String 'The variable for holding the result
Const MaxUsernameLength As Integer = 7

Dim sFirst As String
Dim sInitial As String
Dim sLast As String
Dim sFirstPart As String
Dim sInitialPart As String
Dim sLastPart As String

'
' Remove spaces and hyphens...
'
sFirst = Replace(Replace(Trim(DTM.Source("givenName"))," ",""),"-","")
sInitial = Replace(Replace(Trim(DTM.Source("initials"))," ",""),"-","")
sLast = Replace(Replace(Trim(DTM.Source("sn"))," ",""),"-","")

'
' Construct the logon name...
'
If (Len(sFirst) + Len(sInitial) + Len(sLast)) <= MaxUsernameLength Then
'We don't have 7 characters total, let's go with what we have
sResult = sLast & sFirst & sInitial
Else
If Len(sInitial) > 0 Then
sInitialPart = Left(sInitial,1)
Else
sInitialPart = ""
End If

If Len(sLast) >= 5 Then
sLastPart = Left(sLast,5)
Else
sLastPart = sLast
End If

If Len(sFirst) >= (MaxUsernameLength - (Len(sLastPart) +
Len(sInitialPart))) Then
sFirstPart = Left(sFirst,(MaxUsernameLength - (Len(sLastPart) +
Len(sInitialPart))))
Else
sFirstPart = sFirst
End If

sResult = LCase(sLastPart & sFirstPart & sInitialPart)
End If


'
' Skip this record if the resultant value is a Null string...
'
If sResult = vbNullString Then DTM.CancelRow()

'
' Return the logon name...
'
DTM.Result = sResult
```

Scripting Environments

Synchronize provides two scripting environments. These are:

1. Script Editor
2. Global Script Editor

You have already learnt about the **Script Editor** (SE), in the previous section where you were told how to write a custom transformation script in it. Transformations are applicable at field level, hence its scope is limited to the event that creates or updates the particular field and the SE environment provides the tools specific to this scope.

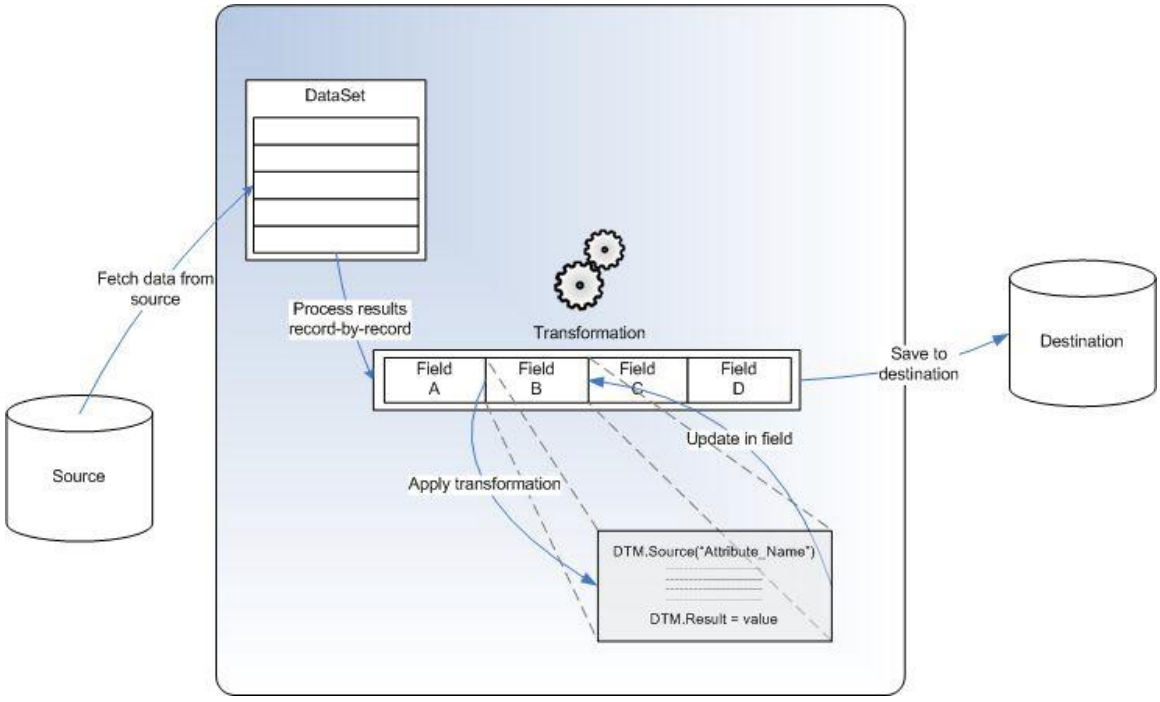


Figure - A higher level representation of the mechanics involved in a transformation.

The Global Script Editor (GSE) is available from the **Connect Synchronized Fields** page of the Synchronize job wizard which is the same page from where you apply transformations. The scope of the script that you write in the GSE is job-wide compared to that written in SE.

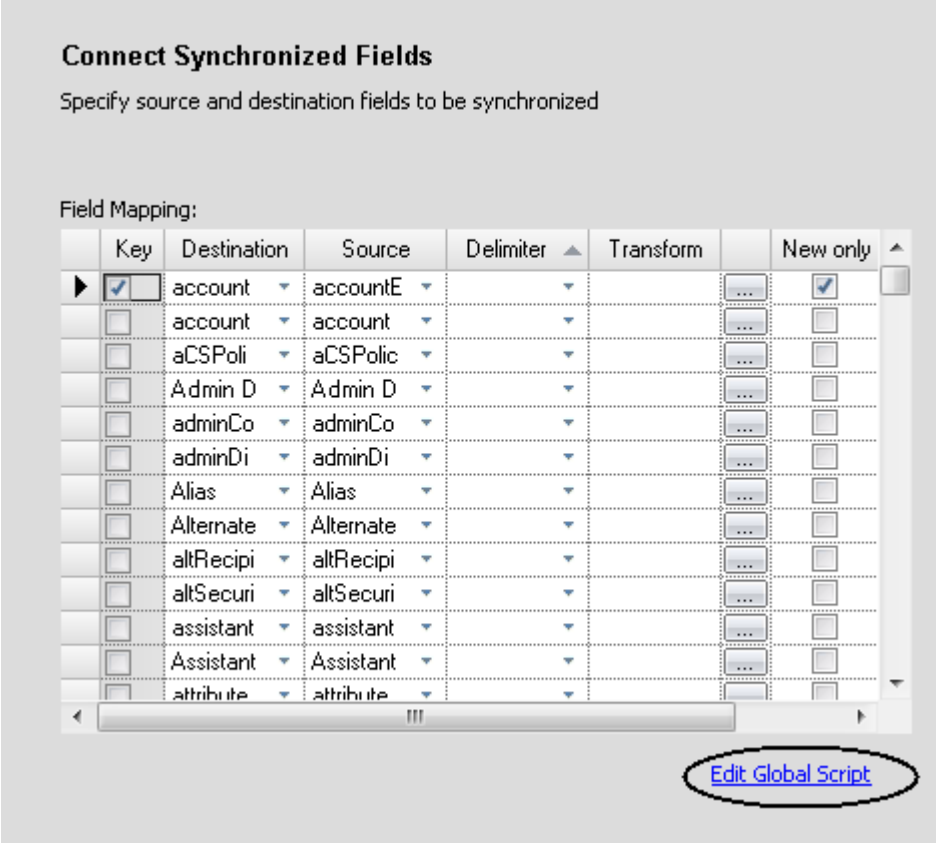


Figure - Shows the link to open the Global Script Editor on Connect Synchronized Fields page of the New Job and Open Job wizard.

In addition to the native DTM object, you can also create objects of the default .NET classes in the System namespace as they are by default referenced by the editor. And if that does not meet your need, you can add references for additional .NET or third party assemblies to use them in your script.

GSE is also intelligent enough to sense the script as you type and displays the list of object properties and functions as well as the help about the parameters that are supposed to be passed to the functions.

DTM Object

DTM Object

The DTM object provides access to the data extracted from the underlying data source. Using the properties and functions exposed by this object, you can manipulate object values within your custom code. This object has the following members:

Properties

- Source
- Result
- ExpandVariables
- Context

Methods

- CancelRow
- AddToContext

Events

- DTM_Startup
- DTM_BuildSourceQuery
- DTM_RowStarting
- DTM_BuildDestinationQuery
- DTM_RowChanging
- DTM_RowChanged
- DTM_RowAdding
- DTM_RowAdded
- DTM_RowDeleting
- DTM_RowDeleted
- DTM_RowFinishing
- DTM_RowFinished
- DTM_RowFailed
- DTM_Shutdown

These are described in the sections that follow.

Properties

Source

Retrieves the value of the specified field name. This is a read-only property and cannot be used for assigning values.

Syntax

```
DTM.Source("Field Name")
```

Example

```
Dim LastName As String = DTM.Source("sn")
```

Result

Returns the referenced string, number or variable value to save it to the destination field.

Syntax

```
DTM.Result string | number | variable
```

Example

```
Dim sAlias As String = "jsmith"
DTM.Result = sAlias
```

ExpandVariables

Returns the value, as a string, of the specified text after replacing each environment variable embedded in the text with the string equivalent of the value of the variable.

Syntax

```
DTM.ExpandVariables("Text")
```

Example

The following code uses the **%SystemDrive%** environment variable to get the system drive letter of the host machine and then concatenates it with the directory path that follows. The result is stored in a string type variable.

```
Dim UserProfile As String = DTM.ExpandVariables("%SystemDrive%" &
"\Documents and Settings\")
```

Context

This is a property with a single argument: Key. Object which has been added to the Context is retrieved by passing its key (identity) to this property.

Syntax

```
DTM.Context("Key")
```

Example

The following code retrieves a DataSet object from the Context and returns the total number of rows for the table at zero-index using DTM.Result.

```
If (DTM.Context("UsersDataSet") IsNot Nothing)
  Dim DS As System.Data.DataSet
  DS = DTM.Context("UsersDataSet")
  DTM.Result = DS.Tables(0).Rows.Count
End If
```

Methods

CancelRow

CancelRow is a DTM function that cancels the update or create action for the current destination row. It provides a way to bypass certain objects based on their attributes.

> For performance reasons, it is preferable to use a filter query to exclude records not to be updated or created.

Syntax

```
DTM.CancelRow()
```

Example

The following code sets the manager attribute for records having department set to Support. For other departments, it will bypass the action.

```
If DTM.Source("department") = "Support" Then
DTM.Result = "Roger Mason"
Else
DTM.CancelRow()
End If
```

AddToContext

This is a function with two arguments: Key and Value. When data is to be shared across segments of code in different editors supported by the Synchronize job wizard, it needs to be placed in the Context.

Syntax

```
DTM.AddToContext("Key", Object)
```

Example

The following code loads an XML file into a DataSet and then adds it to the Context on the Startup event of a Synchronize job.

```
Sub DTM_Startup(dtmsource As Object, args As EventArgs) Handles
DTM.Startup
  ' User-definable script goes here -----------------
  Dim DS As New System.Data.DataSet()
  DS.ReadXML("C:\ADUsers.xml")
  DTM.AddToContext("UsersDataSet",DS)
  ' -------------------------------------------------
End Sub
```

DTM Global Events

The DTM object exposes job and row level events through the Global Script Editor for implementing custom business logic. These events are also called the DTM Global Events and are raised during the execution of a DTM job.

Event	Event is raised
DTM_Startup	as soon as the job starts. Since it is raised at the job start, it requires no previous action to be performed. Any other action that needs to be performed has to be made part of an event that is raised after this one.
DTM_BuildSourceQuery	when the Source Query is analyzed. Source Query contains information about which row(s) or column(s) need to be processed. Selection of the relative data entities raises this event.
DTM_RowStarting	when a complete row is being prepared for copying to the destination.
DTM_BuildDestinationQuery	when the query is generated for copying source data to the destination.
DTM_RowChanging	before updating a record in the destination.
DTM_RowChanged	when changes have been made to the selected attributes' values on the destination side.
DTM_RowAdding	when a new record is to be added in the destination.
DTM_RowAdded	when a new record has been added in the destination.

Event	Event is raised
DTM_RowDeleting	when a record is selected for deletion.
DTM_RowDeleted	when the record has been deleted in destination.
DTM_RowFinishing	when the record copying process is about to finish.
DTM_RowFinished	when the record copying process finishes.
DTM_RowFailed	when a change, add, or delete action on a record fails to execute successfully.
DTM_Shutdown	when the Close (X) button is clicked on the user interface at any stage. This event will not be raised if the job is being executed using the command line.

Context

The Context plays a central role in the Synchronize job model. Since in a Synchronize job, assemblies for Synchronize PowerTools and other third-party libraries can only be referenced in the Global Script Editor, manipulating objects of these libraries in other code segments in a job is only possible by adding them to the Context.

The Context is an implementation of the .NET Hashtable collection which is an in-memory data structure that stores and retrieves objects using key/value pairs. The DTM object in the Synchronize job model provides two members: AddToContext and Context for adding and retrieving objects from the Context respectively. To learn more about these two members, please see the previous section on DTM Object.

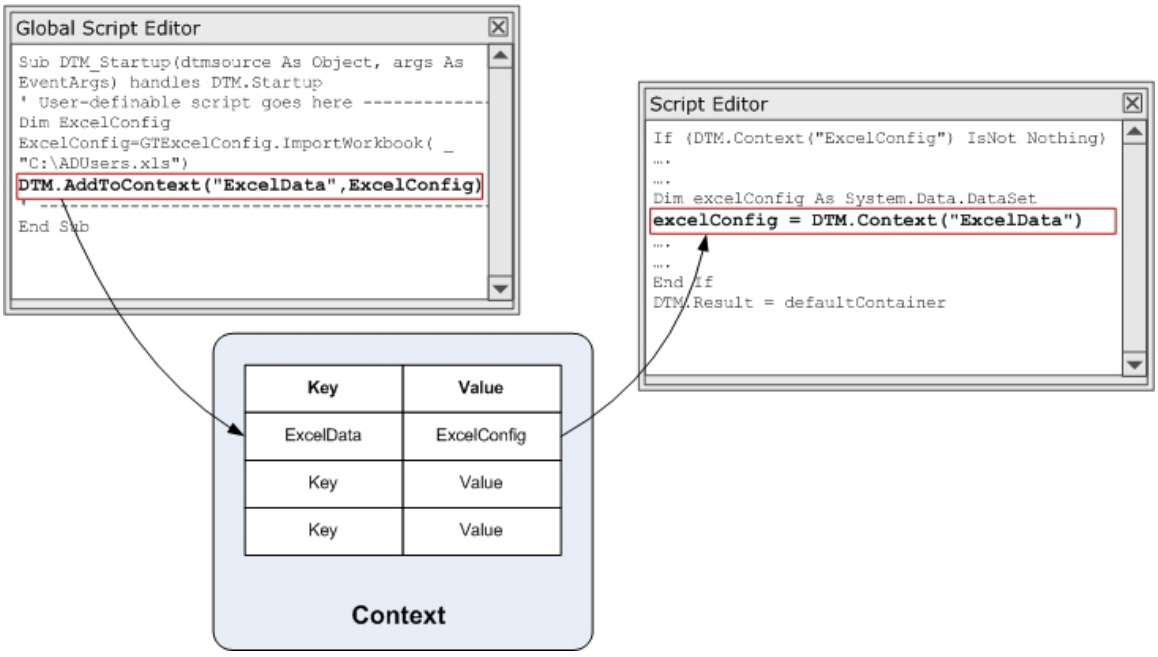


Figure - The use of DTM.AddToContext and DTM.Context members to add and retrieve objects from the Context.

Although a Context makes possible the sharing of objects added to it across different code segments of a Synchronize job, it is not possible to test your code for each segment individually without actually running the job. For this reason, you may find yourself in one of the following situations:

- Receive an exception when trying to compile the code in the Script Editor, stating that the object reference is not found.
- If you have handled the exception in your code and have checks in place for null object references, testing your script using the in-built Script Tester with random data may not provide you with the expected results.

JobEventArgs Class

JobEventArgs is the class containing event data for all Row events in DTM Object. This class has the following members:

Property

- StagingDestination

Method

- SetStagingDestination

StagingDestination

Returns the value of the specified destination attribute.

Syntax

```
StagingDestination("Field Name")
```

Example

See the example for SetStagingDestination.

SetStagingDestination

Sets the value of the specified destination attribute.

Syntax

```
SetStagingDestination("Field Name", "Value")
```

Example

The code in the following example, transforms the middle name of a user to a shorter form. For example, if the middle name is Andrew, it will be changed to "A."

```
Sub DTM_RowAdding(ByVal dtmsource As Object, ByVal args As
JobEventArgs) Handles DTM.RowAdding
  Dim MiddleName As String
  MiddleName = String.Left(args.StagingDestination("middleName"), 1) &
"."
  args.SetStagingDestination("middleName", MiddleName)
End Sub
```

The example demonstrates a scenario where Active Directory is being used as a destination and the middleName attribute amongst the selected fields on the **Select Destination Fields** page of the Job wizard.

The StagingDestination Concept

Staging Destination refers to a stage where destination fields and their values are stored in an in-memory data structure before they are saved at the destination. These destination fields will be those that have been selected on the Select Destination Fields page of the Synchronize Job wizard, see figure below. However, programmatically, more destination fields can also be added using the SetStagingDestination method of the JobEventArgs class provided that they exist on the destination side.

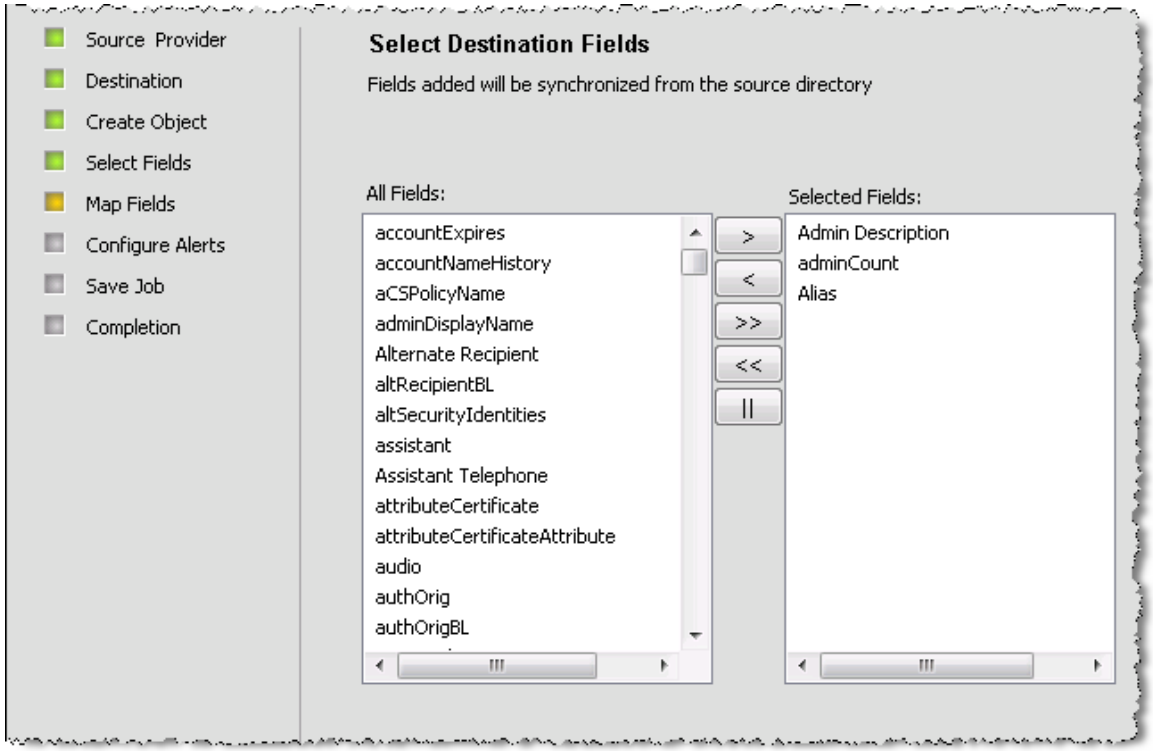


Figure - The Select Destination Fields page. This page is available from both the New Job and Open Job wizards.

Getting Familiar with the Global Script Editor

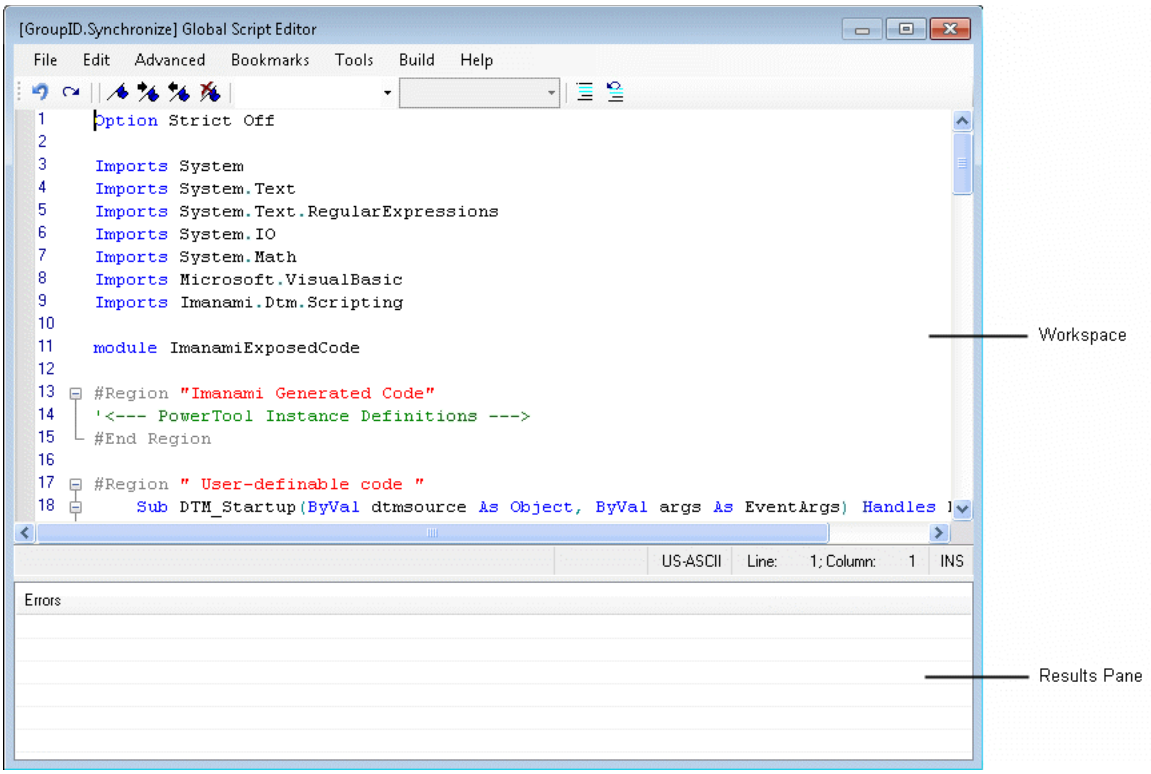


Figure - The Global Script Editor

Menu bar

File Menu

Command	Description
Exit	Closes the editor.

Edit Menu

Command	Description
Cut	Copies the current text selection to the clipboard and deletes the selection.
Copy	Copies the current text selection to the clipboard while keeping the selection.
Paste	Inserts the copied or cut text from the clipboard in the workspace.
Delete	Deletes the current text selection.
Undo	Reverses the last change.
Redo	Re-applies a change reversed using the Undo action.

Command	Description
Find	Opens the **Find** dialog box for searching text in the editor.
Replace	Opens the **Replace** dialog box for searching and replacing text in the editor.
Go To	Opens the **Go To Line** dialog box for jumping to a specific line in the editor.
Select All	Selects all the text in the editor.
Insert File As Text	Opens the **Select a text file** dialog box that allows you to select a text file from which to insert text into the editor.
Time/Date	Inserts the current date and time in the editor.

Advanced Menu

Command	Description
Tabify Selection	Increases indentation of the current text selection.
Untabify Selection	Decreases indentation of the current text selection.
Comment Selection	Comments the current text selection.
Uncomment Selection	Uncomments the current text selection.
Make Uppercase	Converts the current text selection to uppercase.
Make Lowercase	Converts the current text selection to lowercase.
Delete Horizontal Whitespace	Removes horizontal white space characters from the current text selection. Horizontal white spaces include, tabs, spaces, new line characters and similar.
Increase Line Indent	Increases the indenting of the current text selection.
View White Space	Toogles the show, hide behavior for displaying white space characters in the editor.
Incremental Search	Use with **Find** to search for other instances of a string in the editor.

Bookmarks Menu

Command	Description
Toogle Bookmark	Adds a bookmark to the current line, or removes it if already present.
Next Bookmark	Jumps to the next bookmarked line in the editor.
Previous Bookmark	Jumps to the previous bookmarked line in the editor.
Clear Bookmarks	Clears all applied bookmarks.

Tools Menu

Command	Description
Add Reference	Opens the **Add Reference** dialog box for including other .NET assemblies in the project.

Build Menu

Command	Description
Compile Script	Checks the script for errors and compiles it.

Help Menu

Command	Description
Contents	Opens the help for GroupID.
About	Opens the **About Imanami Synchronize** dialog box.

Toolbar

Figure - The Global Script Editor toolbar.

Button	Description
	Reverses the last change.
	Re-applies a change reversed using the Undo action.

Button	Description
	Adds a bookmark to the current line, or removes it if already present.
	Jumps to the next book-marked line in the editor.
	Jumps to the previous book-marked line in the editor.
	Clears all applied bookmarks.
	Shows the list of global objects.
	Comments the current text selection.
	Un-comments the current text selection.

VB Options Set by Synchronize

Synchronize establishes the following Option statements. These options apply to all scripts and cannot be overridden:

- **Option Explicit On** - all variables must be declared before use via a Dim statement. With VB.Net, it is possible to both declare and assign variables at their first use, as in:

```
Dim MyVariable = "Hello"

Dim MyObject = new Object()
```

- **Option Strict Off** - datatypes don't need to be declared for each variable. Conversions between types, when possible, are performed implicitly. (By declaring datatypes, unnecessary conversions can be avoided, and performance improved).

Scripting Restrictions by Synchronize

Behind the scenes, Synchronize inserts each script into the body of a subroutine before compiling. Therefore, any Visual Basic.Net constructs that are only valid outside of a subroutine/function will fail to compile and will be disallowed.

When creating a Synchronize script, the following restrictions apply:

- Subroutines, functions, classes, modules, namespaces are not allowed.
- Module-level statements, such as Import or Option statements, are not permitted.
- Shared (i.e., static, global) variables are not supported.

.Net Assembly References

Synchronize establishes certain system assembly references before compiling your scripts. These references apply to all scripts and cannot be overridden. These references are:

- MsCorLib.dll

- System.dll
- System.Data.dll
- System.Xml.dll

System.DirectoryServices, in particular, is "off-limits" to your scripts. This prevents direct access to Active Directory and other LDAP data stores. This is a desirable restriction, as it prevents your script from acting in conflict with Synchronize – which, after all, has final responsibility for updating these data stores.

.Net Namespaces

Synchronize imports certain namespaces when compiling your scripts. These imports apply to all scripts and cannot be overridden. These imports are:

- Imports System
- Imports System.Text
- Imports System.Text.RegularExpressions
- Imports System.IO
- Imports System.Math

.Net namespaces other than those listed here can still be accessed by specifying the fully-qualified namespace. For example, a DataSet (which belongs to the System.Data namespace) can be read from a file as follows:

```
Dim ds = New System.Data.DataSet()

ds.ReadXml("C:\Temp\MyFile.xml")
```

Chapter 18: Synchronize Options

This chapter looks at the options available for different Synchronize settings. It covers the settings available on the **Options** dialog box for Synchronize. This chapter is divided into the following sections:

Customizing the Job Run Chart, covers the option for setting the number of Jobs to show on the Job Run chart.

Setting the Columns to Display for a Job, covers the option for setting the columns to display for a Job in the All Jobs view.

Setting the Columns to Display for Jobs History, covers the option for setting the columns to display for a Job in the Jobs History view.

Setting the History Threshold Value, covers the setting that controls the number of data items to send to the GroupID Data Service in a single call.

Delimiters, covers the option for managing characters to use as delimiters when mapping multi-value fields using the New Job and Open Job wizards.

Customizing the Job Run Chart

The number of Jobs shown on the Job Run chart are by default set to five. This is also the minimum limit of Jobs that can be set for the chart. The maximum number of Jobs that can be set for the chart are 15. To change the default setting for the chart, use the instructions given in the following:

1. Click the **Synchronize** node in the tree view.
2. Right-click and then click **Options**.
   This opens the **Options** dialog box.
3. On the **Options** dialog box, expand the **Synchronize** node (if not already expanded) and then click **Chart**.
4. In the given field, replace the existing value (by default 5) with a number within the range 5 to 15. Precede values less than 10 with a zero, for example: 05, 06, 07 and similar.
5. Click **OK**.

Setting the Columns to Display for a Job

1. In the GroupID tree view, right-click the **Synchronize** node and then click **Options**.
2. On the **Options** dialog box, expand the **Synchronize** node, if not already expanded, and then click **Job List**.
3. From the given list, select or clear the check boxes for the columns that you want to display or hide in the All Jobs view.
4. Click **OK** to save your changes.

Setting the Columns to Display for Jobs History View

1. In the GroupID tree view, right-click the **Synchronize** node and then click **Options**.
2. On the **Options** dialog box, expand the **Synchronize** node, if not already expanded, and then click **History List**.
3. From the given list, select or clear the check boxes for the columns that you want to display or hide in the Job History view.
4. Click **OK** to save your changes.

Setting the History Threshold Value

History for a Synchronize job includes data about records and attributes that are added, deleted or modified by the job. Since job history is maintained in the central GroupID database, every change in records or attributes during job run is forwarded to the GroupID Data Service which stores it into the database. Under the default settings, a call is made to the data service for each change as it occurs during the processing. For jobs that may process thousands of objects, such frequent calls may result in network congestion and slow down its performance. The threshold value setting, lets you set the number of data items to send in a single call to the data service. A reasonable set of data items will not only lower the network load, but will also improve the database performance.

To set the history threshold value:

1. In the GroupID tree view, right-click the **Synchronize** node and then click **Options**.
2. On the **Options** dialog box, expand the **Synchronize** node, if not already expanded, and then click **History Threshold Value**.
3. In the given box, enter a number within the range of 1 to 500 which determines the number of data items to deliver in a single call to the GroupID Data Service.
4. Click **OK** to save changes.

Delimiters

Delimiters are used in Synchronize Jobs when mapping fields that can have multiple values. By default, there are no characters defined as delimiters in GroupID. To use delimiters, you must first specify one or more characters that you would be using as delimiters. Use the following instructions for this:

1. Click **Synchronize** in the tree view.
2. Right-click and then click **Options**.
   This opens the **Options** dialog box.
3. On the **Options** dialog box, expand the **Synchronize** node (if not already expanded) and then click **Delimiter**.
4. In the given box, type the character to use as delimiter, and then click **Add**.
   The specified character will be added to the delimiters list.
5. Repeat step 4 to add more characters, if required.

The characters added to the list will be available from the **Delimiter** list on the **Map Fields** page of the **New Job** / **Open Job** wizard.

Part 5 - Reports

This part of the documentation covers the Reports module of GroupID. It provides a list of reports that you can run on the Active Directory and Microsoft Exchange and provides instructions on generating them.

Chapter 19: Introduction, provides an overview of Reports and introduces you to different report categories and the output formats.

Chapter 20: Working with Reports, provides step-by-step instructions on generating reports.

Chapter 19: Introduction

This chapter provides a brief overview of Reports and gets you familiar with its user interface. Reports distribution into different categories and their output formats are also covered here. The chapter is divided into following sections:

Overview, provides an overview of Reports.

Getting Familiar with the User Interface, introduces you to the Reports user interface.

Report Categories, covers report distribution into different report categories.

Output Formats, lists the supported output formats for displaying reports.

Overview

GroupID Reports empowers administrators to analyze and monitor Active Directory and Exchange server activities and collect statistical information about critical objects, thus enabling you to have an up-to-date picture of your directories and servers. The module primarily focuses on groups and distribution lists allowing administrators to list their members, owners, last modified time and so on. It also enables them to view the list of all users, workstations, domain controllers along with their operating systems within an organization. The module provides complete flexibility to customize the format, scope and layout of reports according to your requirement.

Getting Familiar with the User Interface

GroupID Reports is a **Free** module and will be available even if you do not have a license for any GroupID module. In the GroupID Management Console, the **Reports** node appears below **Password Center**. Expand the Reports node to view its sub-nodes. The sub-nodes categorize reports into two views: **All Reports** and **By Category**. All Reports view shows all available reports; and By Category view distributes reports into different categories. For information about these categories, see **Report Categories** later in this chapter.

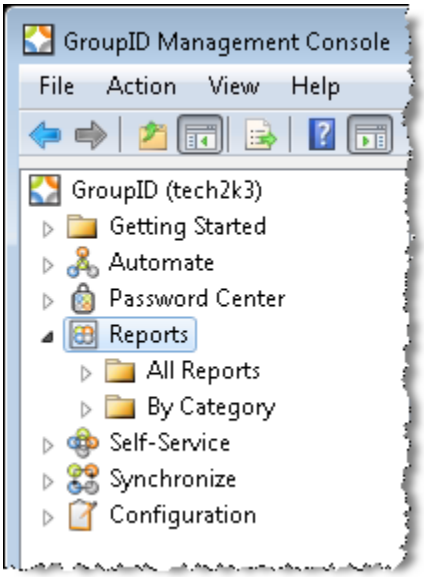


Figure - The Reports node

Report Categories

Reports module divides all reports into four different categories:

1. Groups
2. Users
3. Computers
4. Contacts

The distribution of reports into these categories is based on the type of data they report. Due to this reason a report may appear in more than one category. For example; the **Mail-enabled groups and members (Exchange)** report is available both under the **Groups** and **Users** categories. Since the report provides information on mail-enabled groups in an Exchange organization, it is available in the Groups category and since it also provides information on the members of mail-enabled groups, it is also available in the Users category.

Following is the summary of reports distribution according to their categories:

	Category	Report	Description
1.	Groups	Deleted groups	Provides a list of logically deleted groups. Logically deleted groups are those expired groups that are not renewed within the time interval set in the global configurations.
		Distribution lists with no delivery restrictions (Exchange)	Provides a list of groups that can receive mail from everyone.
		Expired groups	Provides a list of groups that are either expired automatically by the Group Management Service according to their associated expiration policy or are forcibly marked as expired by users.
		Expiring groups	Provides a list of groups that are approaching their expiry date.
		Groups and members	Provides a list of members for each group in the directory.
		Groups and number of members	Provides a count of total members per group.
		Groups and owners	Provides a list of owners and the groups they own.
		Groups and their last modified time	Provides the date and time of the last change made to a group. Such as modifying membership.
		Groups that have no members	Provides a list of groups without members.
		Groups with no owner	Provides a list of groups that are not managed by an owner.
		Mail-enabled groups and members (Exchange)	Provides a list of groups and members that are mail-enabled.
		Mail-enabled groups and number of members (Exchange)	Provides a list of groups and the count of members they have.
		Mail-enabled groups and owners (Exchange)	Provides a list of all mail-enabled groups and their owners.
		Mail-enabled groups and their	Provides a list of all mail-enabled groups and the

	Category	Report	Description
		last modified time (Exchange)	date and time when they were last modified.
		Mail-enabled groups with no members (Exchange)	Provides a list of mail-enabled groups having no members.
		Mail-enabled groups with no owner (Exchange)	Provides a list of mail-enabled groups having no owner.
		Mail-enabled Recipients and the groups they are members of (Exchange)	Provides a list of all mail-enabled recipients and the groups that they hold membership of.
		Recipients and the groups they are a member of	Provides a list of users and each group that they are a member of.
		Owners and objects they own	Provides a list of managers and their direct reports.
2.	Users	Disabled Users	Provides a list of accounts with no authentication access to mail or computers in an organization.
		Mail-enabled groups and members (Exchange)	Provides a list of groups and members that are mail-enabled.
		Mail-enabled groups and owners (Exchange)	Provides a list of all mail-enabled groups and their owners.
		Mail-enabled Recipients and the groups they are members of (Exchange)	Provides a list of all mail-enabled recipients and the groups that they hold membership of.
		Mail-enabled users and contacts with a phone number (Exchange)	Provides a phone list of accounts within an organization for only mail-enabled users and contacts.
		Owners and objects they own	Provides a list of managers and their direct reports.
		Recipients and the groups they are a member of	Provides a list of users and each group that they are a member of.
		Users and contacts with a phone number	Provides a phone list of accounts within an organization.
		Users who are locked out	Provides a list of accounts that have been denied access to their computer.
3.	Computers	Computers and operating system	Provides a list of workstations and domain controllers within an organization.
		Computers running Window 2000 Professional	Provides a list of computers in the network running Windows 2000 Professional.

	Category	Report	Description
		Computers that have never logged on to the network	Provides a list of computers that have never logged on to the network.
		Computers with Windows 2000 (Non Domain Controllers)	Provides a list of computers running Windows 2000 and that are not promoted as Domain Controllers in the network.
		Computers with Windows 2003 (Non Domain Controllers)	Provides a list of computers running Windows 2003 and that are not promoted as Domain Controllers in the network.
		Computers with Windows NT 4.0 (Non Domain Controllers)	Provides a list of computers running Windows NT 4.0 and that are not promoted as Domain Controllers in the network.
		Computers with Windows XP	Provides a list of computers running Windows XP in your network.
		Disabled computers and their operating system	Provides a list of workstations and domain controllers that have been retired within an organization.
		Domain Controllers running Windows 2000	Provides the list of Windows 2000 Domain Controllers running in your network.
		Domain Controllers running Windows 2003	Provides the list of Windows 2003 Domain Controllers running in your network.
		Domain Controllers running Windows NT	Provides a list of Domain Controllers running Windows NT in your network.
4.	Contacts	Users and contacts with a phone number	Provides a phone list of accounts within an organization.

Output Formats

Reports module supports different formats for displaying outputs of a particular report. These output formats vary according to the report you are generating and not all formats may be supported for every report. Output formats supported by GroupID for reports are:

- Web Page (HTML)
- Microsoft Excel (XLS)
- Comma Separated Value (CSV)
- Extensible Markup Language (XML) Format

Chapter 20: Working with Reports

This chapter provides information on report build criteria and its manipulation. The chapter is divided into following sections:

Generate a New Build Criteria, provides information on creating a new build criteria using the Create Report wizard.

Report Files, explains in detail the different files created for a report and where they are located.

Generate Report from Build Criteria, explains how you can generate report from an existing criteria.

Reports Command-line Utility, explains how you can use Reports command-line utility to generate report.

Edit Report Build Criteria, explains how you can change a report build criteria.

Delete Build Criteria, provides instructions on deleting a build criteria.

Scheduling, describes how you can auto-generate reports by defining scheduled jobs for them.

Generate a New Build Criteria for Report

A build criteria of a report comprises of following things:

1. Output format
2. Scope in Active Directory
3. Output fields
4. Sort-by field
5. Report title
6. Location on the disk

Reports provides a simple and user-friendly wizard to build the report criteria. Once this criteria is built, you can use it any time to generate reports quickly.

The instructions below describe the procedure of creating new build criteria for the **Groups and owners** report. Same instructions apply to creating reports of all types.

1. On the GroupID Management Console, expand the **Reports** node.
2. Under the **By Category** node, expand the **Groups** node.
3. Right-click **Groups and owners** and click **Create Report**. This starts the **Create Report** wizard.
4. On the **Introduction** page, read the welcome message and click **Next**.

Create Report
Introduction
Select View
Define Scope
Edit Report Fields
Select Sort Field
Customize Report
Review Selections
Running Report
Completion
Introduction
Welcome to GroupID Smart Reports.
Smart Reports (Reporting) is a reporting tool designed to run reports on the Microsoft Active Directory directory services. This version of GroupID Reporting focuses on distribution lists and groups allowing the user to list all the members of a group, the owner, last modified date and more.
The GroupID Reporting wizard will now walk you through building a report.
Help
Next >
Cancel

Figure - The Introduction page

5. On the **Select View** page, select the required output format and click **Next**. For more information about output formats, see **Output Formats** in **Chapter 19: Introduction**.

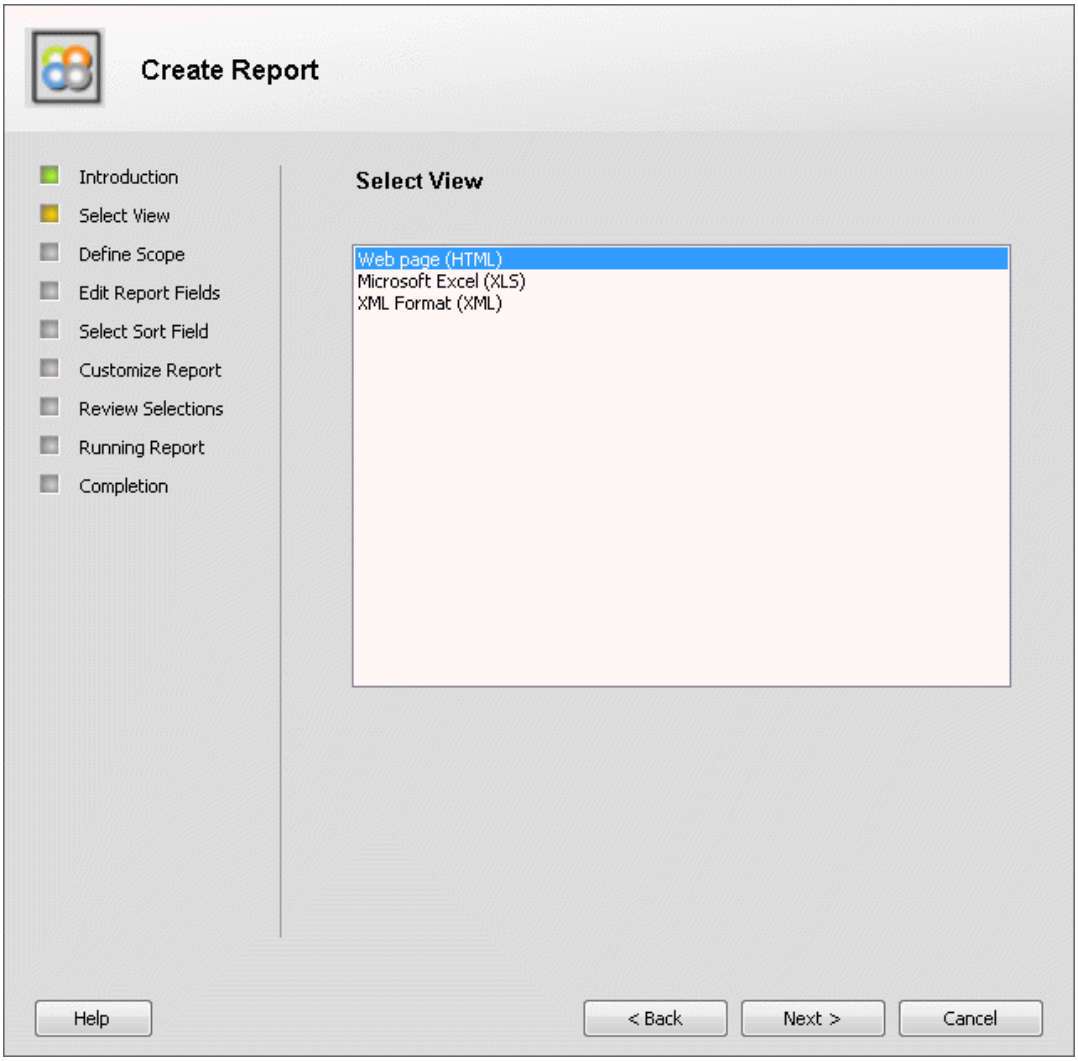


Figure - The Select View page

6. By default, the wizard searches the Global Catalog for generating the report output. On the **Define Scope** page, you can limit this scope to a particular container. To do this:

    i. Click **Browse** to open the **Select Container** dialog box and select the required source container.

    ii. You can select the **Include sub containers** check box to also include sub-containers for the selected container when reporting.

    iii. In the **Edit criteria** box, modify the default LDAP filter as required. This filter is used for selecting items from the selected container that matches the given criteria.

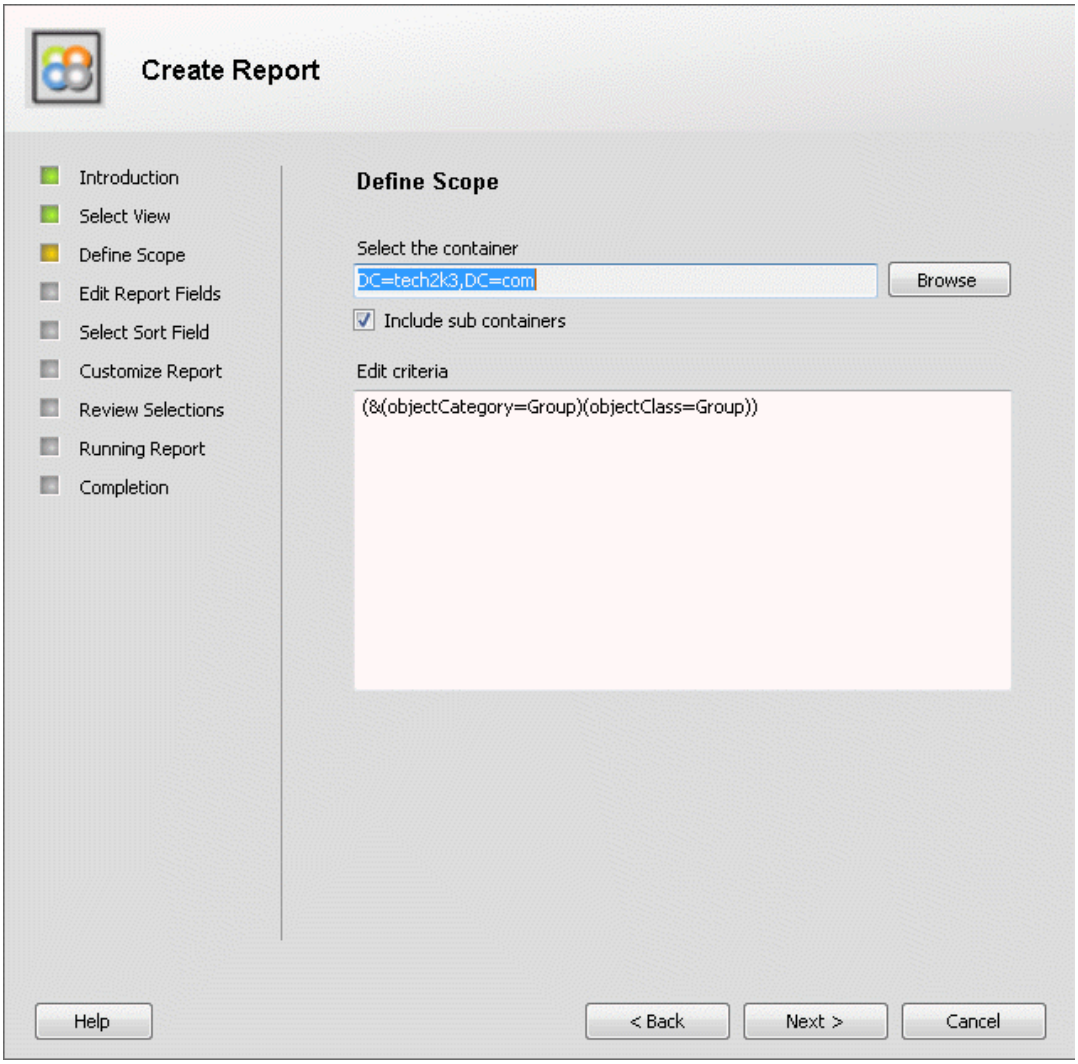


Figure - The Define Scope page

7. Click **Next**.

If no groups are found within the specified scope, the wizard will prompt you as soon as you click **Next**.

8. The **Edit Report Fields** page shows the list of default fields that will be included in the report output. Some of the fields may also have sub-fields. For example, expanding the **Owner** field shows the **Name, Office** and **E-mail** sub-fields. These sub-fields are represented in different output formats as follows:

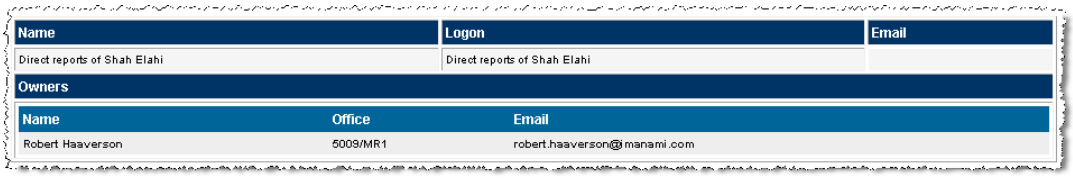


Figure - The representation of sub-fields in Web page output format

Name	Logon	Email	Owners		
Direct reports of Shah Elahi	Direct reports of Shah Elahi				
			Name	Office	Email
			Robert Haaverson	5009/MR1	robert.haaverson@imanami.com

Figure - The representation of sub-fields in Microsoft Excel output format

To add more fields in the report output, click **Add**. This displays the **Add a Field to the Report** dialog box where you can select the source field and provide a display name for the field. You can also remove a field from the output by selecting it and clicking **Remove**. You can change the order of these fields by using **Move Up** and **Move Down**.

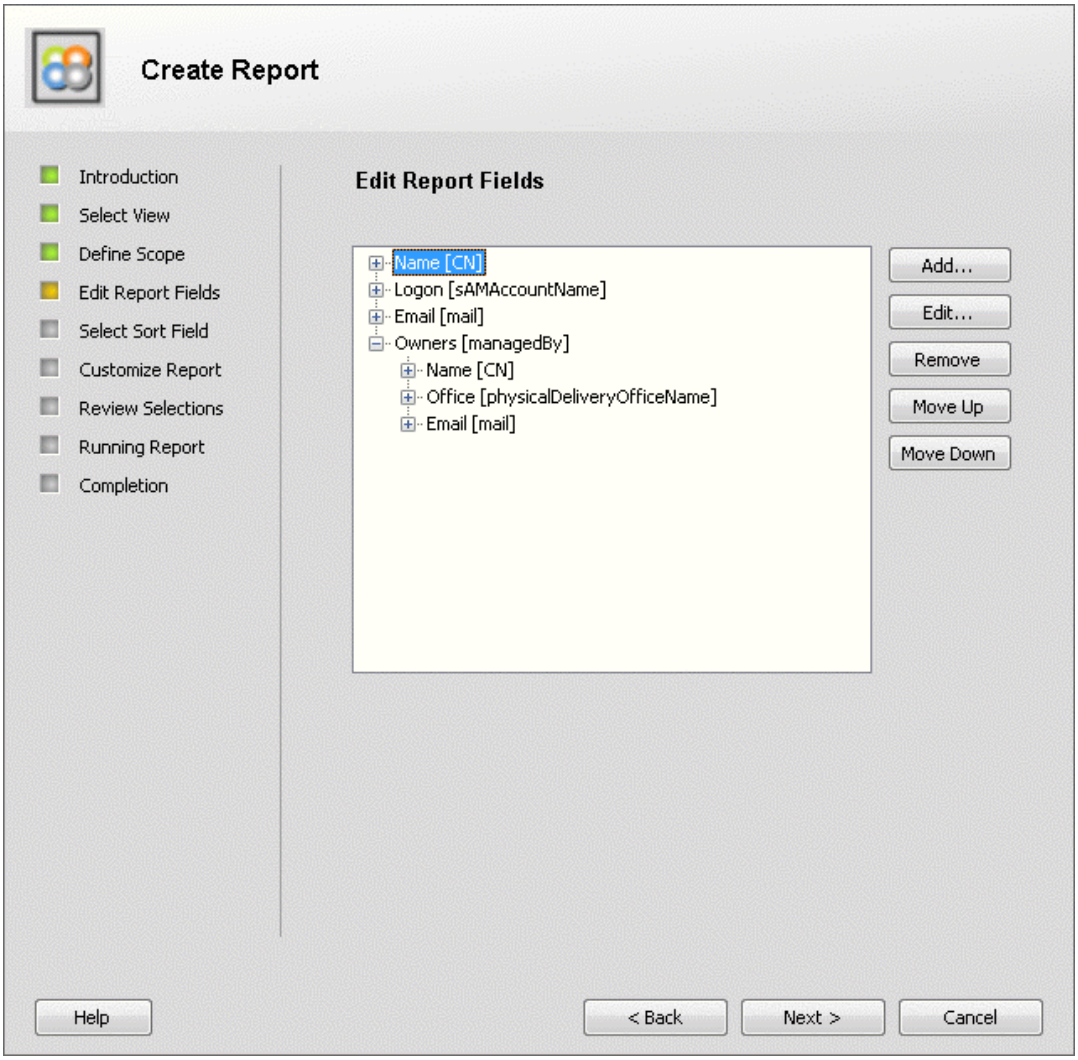


Figure - The Edit Report Fields page

9. Click **Next**.
10. On the **Select Sort Field** page, select the field by which you want to sort the results on the report.

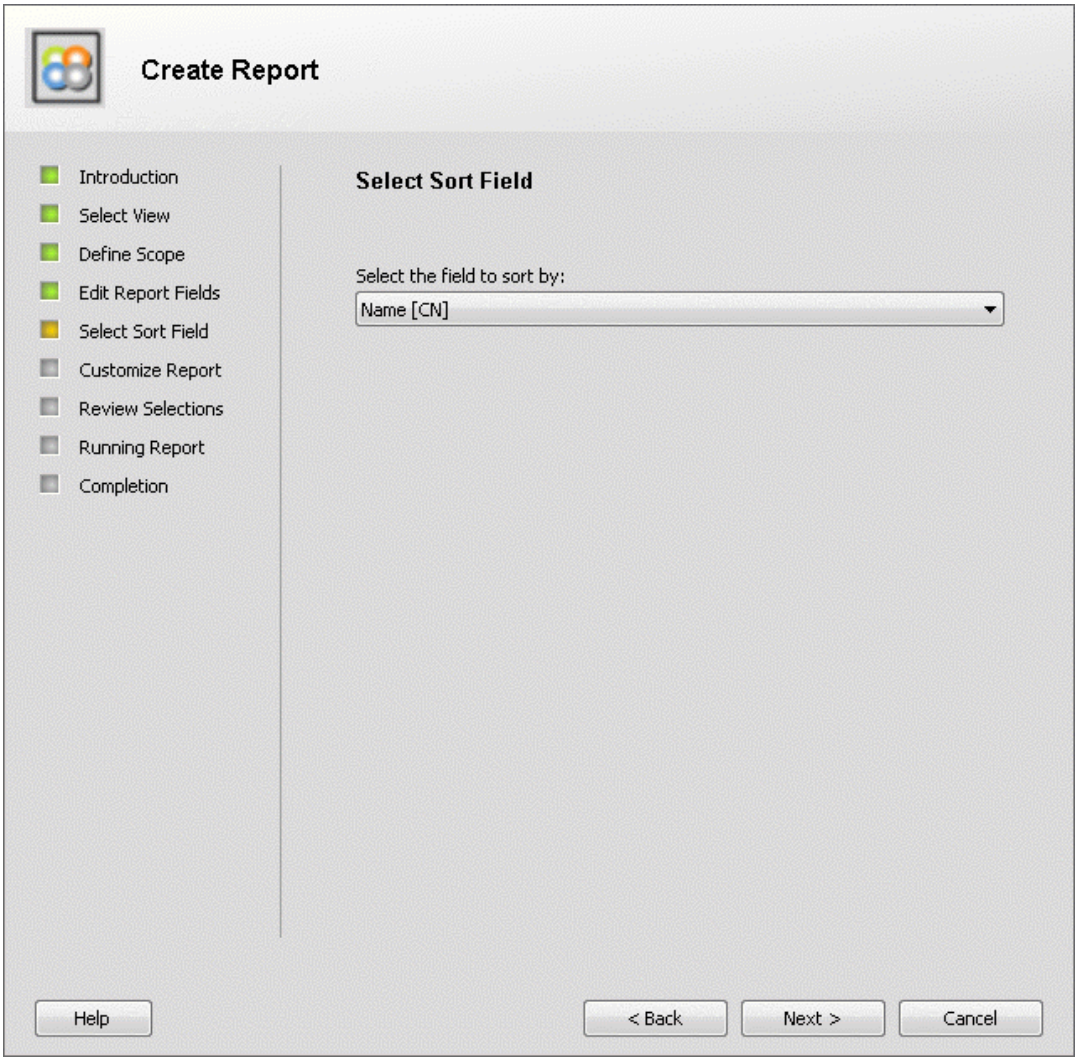


Figure - The Select Sort Field page

11. Click **Next**.

12. On the **Customize Report** page, specify a custom title and the location where you want to save the report's output. Click **Next** to continue to the next step if you are okay with the default settings on this page, else do the following:

    i. To specify a custom title for your report, in the **Report title** box, type the title of the report replacing the existing one.

    ii. The **Save report** box shows the location where Reports will save the generated report. Click **Browse** to select a different location where you want to save the report.

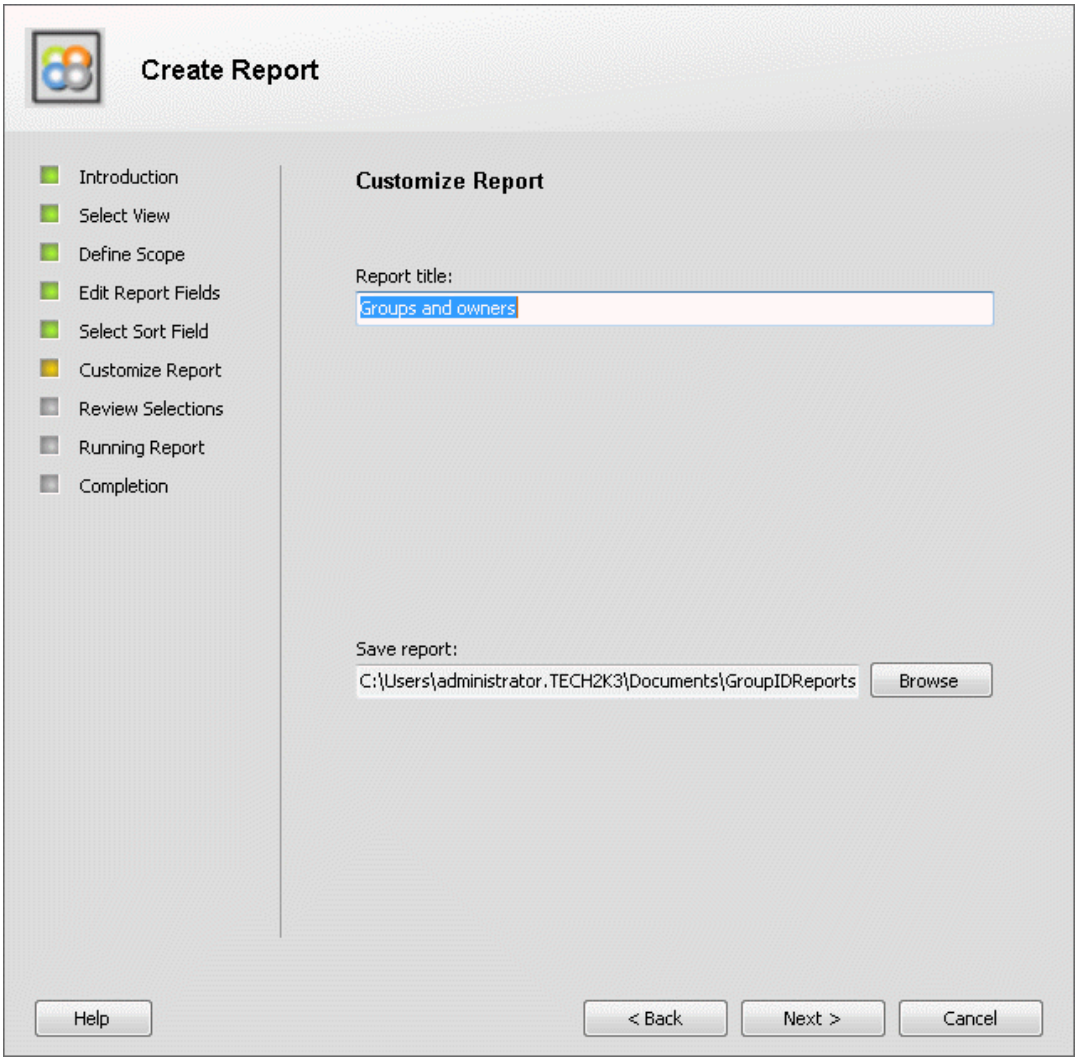


Figure - The Customize Report page

13. Click **Next**.

14. The **Review Selections** page shows the summary of the selections made in the previous steps. On this page:

    i. Click **Next** to generate the report with the existing settings.

    ii. Click **Back** to go to a previous screen and make changes.

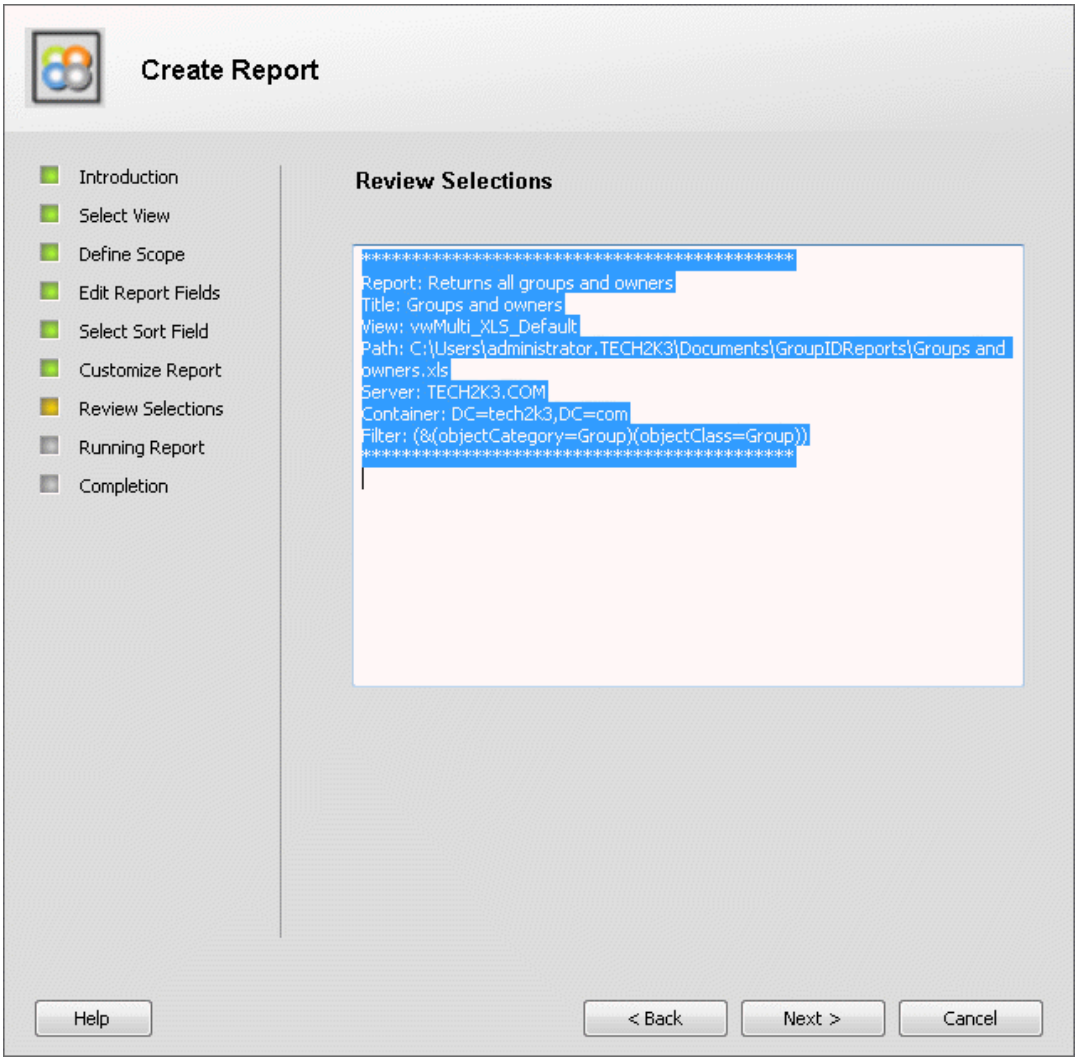


Figure - The Review Selections page

15. Once the wizard completes, click **Finish**. This will open your generated report in the output format you selected in the step 5.

Report Files

In addition to the report file, containing all the data, there are two additional files generated by Reports that are saved at the same location as the original report. These files include, the:

1. Snapshot file
2. Options file

The report snapshot file

The report snapshot file is created when a build criteria is run to generate the report. This file is saved with the **.ReportSnapShot** extension and it contains the records retrieved by the report from Active Directory at a particular time stamp.

Reports creates a new snapshot file every time a build criteria is run and archives it.

The report options file

This is the main file that contains all the settings for a report that you provide to the wizard when creating or modifying it. This file is saved with the **.ReportOption** extension.

Generate Report from Build Criteria

Reports keeps a log of every distinct criteria that you build for generating reports. You can simply run this criteria and Reports will extract data from the directory according to the filters of the criteria and display the report in the output format selected for the criteria.

Use the instructions below to run the criteria that you have created in the **Generate a New Build Criteria** section.

1. On the GroupID Management Console, expand the **Reports** node.
2. Under the **By Category** node, expand the **Groups** node.
3. Click **Groups and owners**.
4. Right-click the criteria and click **Run**. This generates the report according to the criteria.
5. When completed, Click **Finish** to open the report.

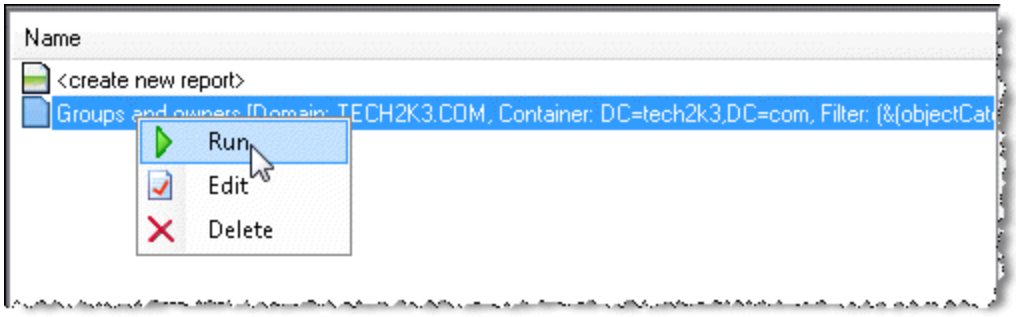


Figure - Run command on the shortcut menu

Reports Command-line Utility

The command-line utility for Reports is designed to facilitate generating reports using the Windows command prompt; provided you have created a build criteria and generated report from that criteria at least once. When you create a new build criteria for generating a report, it is stored in a separate file at the same location where you save the report. The file is named as: ***Report Title*(*Domain name*).ReportOption**. Reports command-line utility requires this file to generate the report. For information about where this file is located, see **Report Files** earlier in this chapter.

Reports command-line utility is available in the installation directory for GroupID by the name **Imanami.GroupID.Reporting.exe**.

To generate a report using this command-line utility:

1. On the command prompt, move to the installation directory for GroupID. By default, GroupID is installed to the location: **C:\Program Files\Imanami\GroupID**.
2. Type the following command:

```
Imanami.GroupID.Reporting /RunReportOptionQuietly "path of the
report options file\report options file name.ReportOption"
```

3. Press **Enter** to run the command.

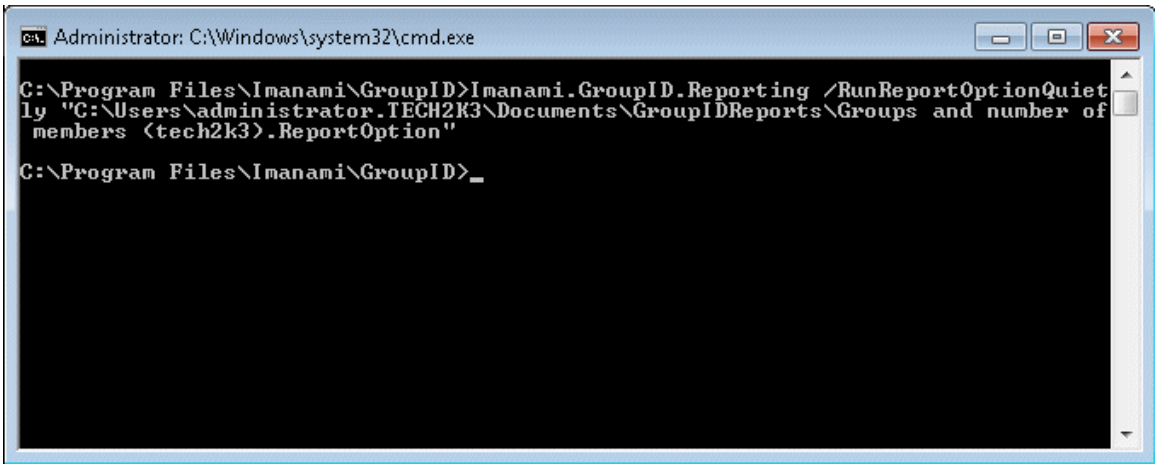


Figure - the command prompt showing the command to generate the report

To verify that the report has been successfully generated, open the directory where the report is saved. Here you will notice the following:

1. A new report snapshot file is created with the name: ***Report Title Time stamp when the report is run*.ReportSnapShot**.
2. When you open the report file, the **Run date** shows the latest time stamp when the report is run.

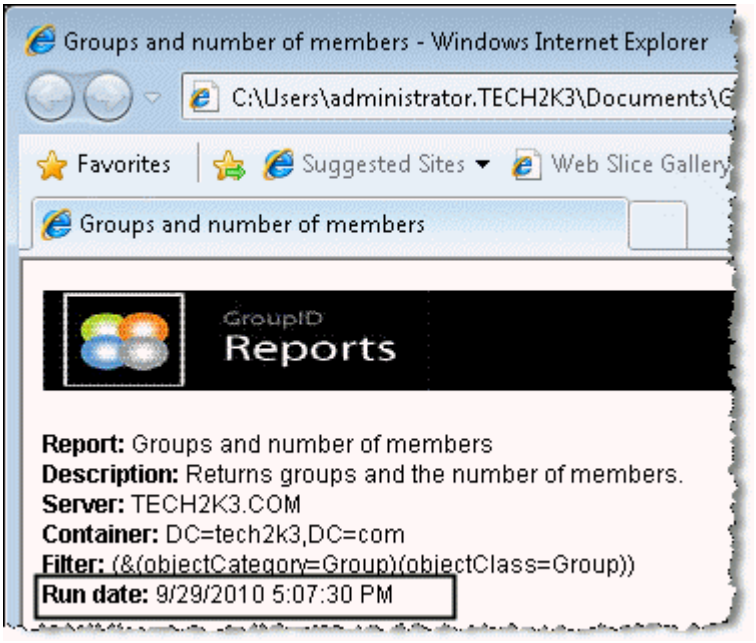


Figure - Run date in the report file

Edit Report Build Criteria

If you have built criteria for the **Groups and owners** report that sorts it by the **Name** field and now you want to sort the report by the **Logon** field for every next run, you can simply change this build criteria accordingly.

To do this:

1. On the GroupID Management Console, expand the **Reports** node.
2. Under the **By Category** node, expand the **Groups** node.
3. Click **Groups and owners**.
4. Right-click the criteria and click **Edit**. This will start the **Create Report** wizard with the criteria settings selected by default. You can change any portion of the criteria on the wizard pages. For more information about manipulating the wizard, see **Generate a New Build Criteria**.

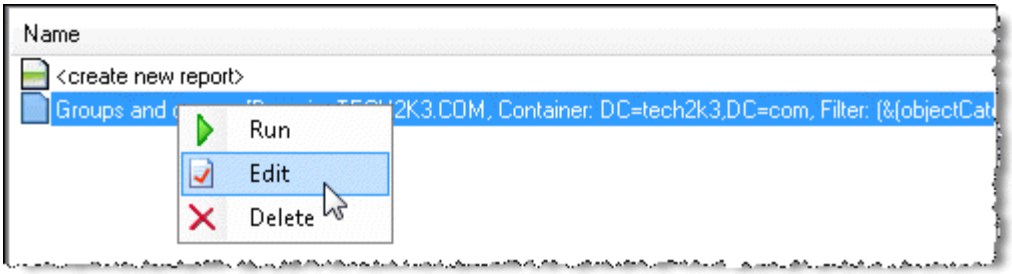


Figure - The Edit command on the shortcut menu

Delete Build Criteria

You may delete criteria if it is no longer required. The following instructions list the procedure for deleting a build criteria.

1. On the GroupID Management Console, expand the **Reports** node.
2. Under the **All Reports** node, click the required report.
3. Right-click the criteria that you want to delete and click **Delete** and then click **Yes** to confirm the deletion.

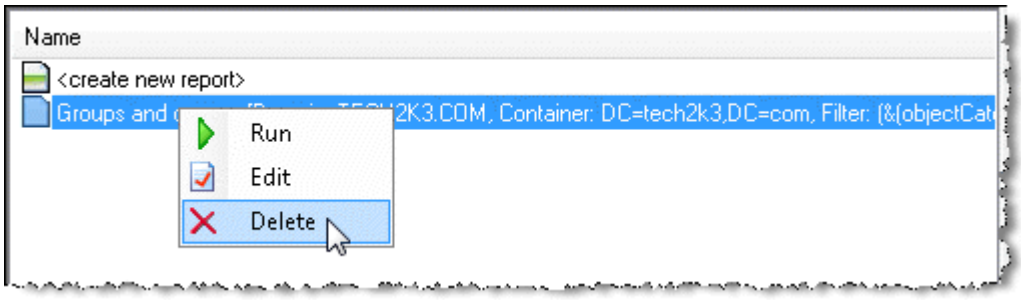


Figure - The Delete command on the shortcut menu

Scheduling Reports

Using GroupID, you can generate reports automatically on scheduled basis. This auto-generation functionality is achieved by creating scheduled jobs. A scheduled job is composed of the following items:

	Job Item	Description
1.	Schedule	A schedule defines the frequency, date and time when the job will execute to generate reports. For example, you can schedule a job to run Daily at 10:00 AM starting from the date January 01, 2009 to December 31, 2009.
2.	Reports	This list of reports criteria that will be processed by the job.
3.	Credentials	A job requires credentials to connect to the domain for getting the latest information.

You create the scheduled job once by adding one or more report criteria to it and afterwards, it runs automatically as per the schedule. During the job run, the reports engine gets the latest information from Active Directory based on the reports criteria and generates reports accordingly. You can also disable a reports scheduled job any time. When the job is needed again, it is as simple as enabling it. If a job is no longer needed, you can remove it.

The report scheduling setting is available when you right-click the **All Reports** node and click **Scheduling Reports**.

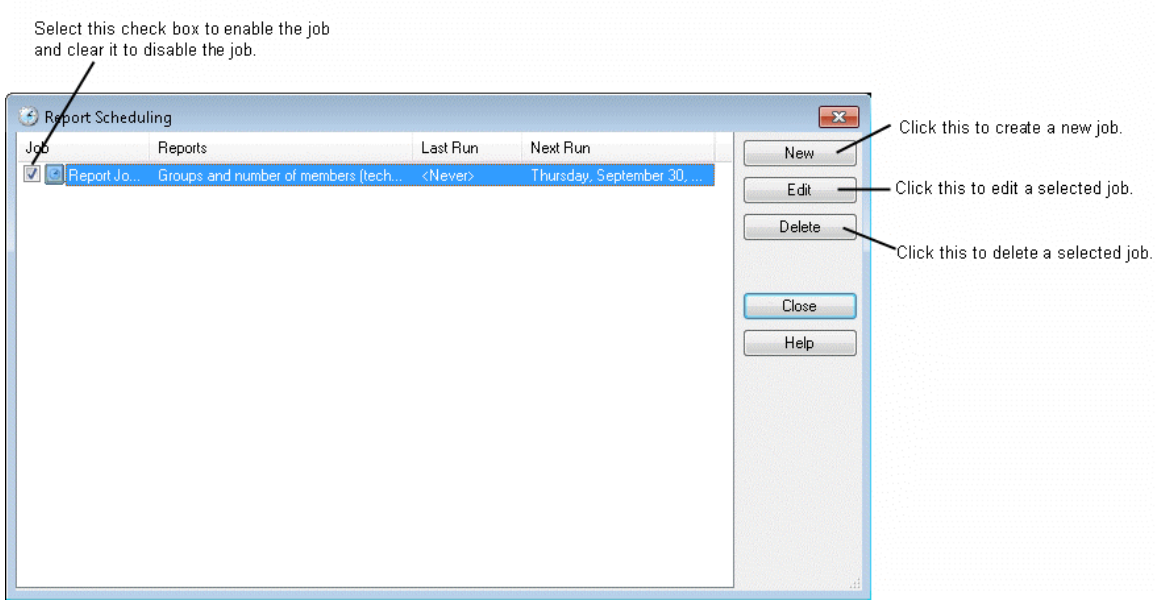


Figure - The Report Scheduling dialog box

Creating a scheduled job

1. On GroupID Management Console, expand the **Reports** node.
2. Right-click **All Reports** and then click **Scheduling Reports**.

3. On the **Report Scheduling** dialog box, click **New**.
   This displays the New Report Job dialog box.

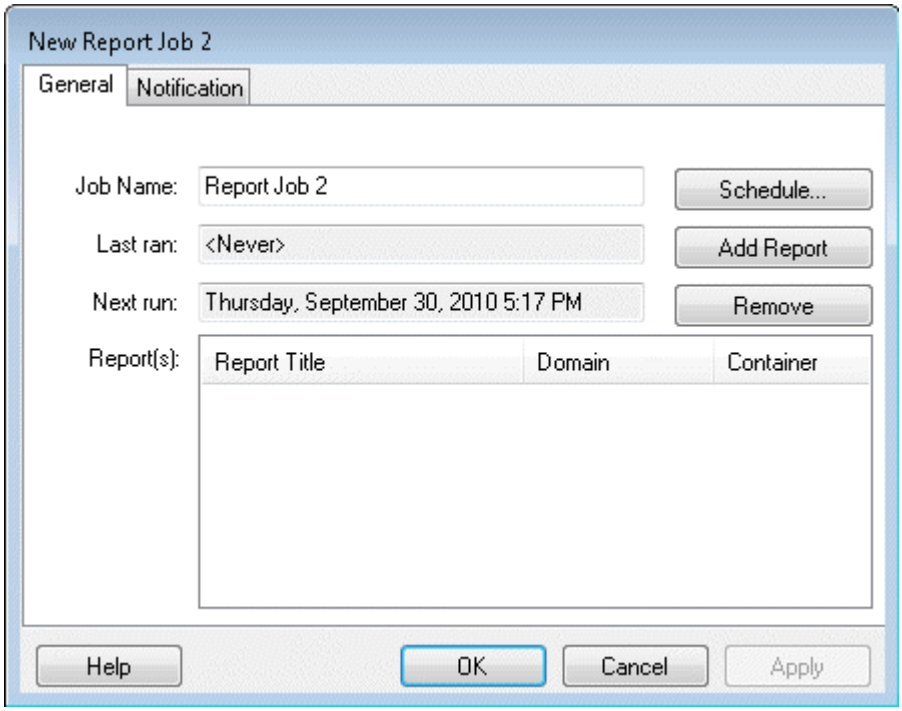


Figure - The New Report Job dialog box - General tab

4. On the **General** tab of the New Report Job dialog box, if provide the following information:

   i. In the **Job Name** box, type the name of the job.
   By default, the box displays a system suggested job name. You can either use this name or enter a different one.

   ii. Click **Schedule** to display the dialog box where you can define the start date, time, frequency and other preferences for the schedule.

   iii. Click **Add Report** to display the **Select Report** dialog box, where:

      a. In the **Report Type** box, type or select a report category.

      b. In the **Report Names** box, type or select the report name.

      c. The **Reports** list shows all criteria that are defined for the selected report. From this list, select one or more reports criteria for the job. To select multiple criteria, hold down the **CTRL** key and click individual criterion, or hold down the **SHIFT** key and select a range of criteria.

      d. Click **OK** to close the dialog box.

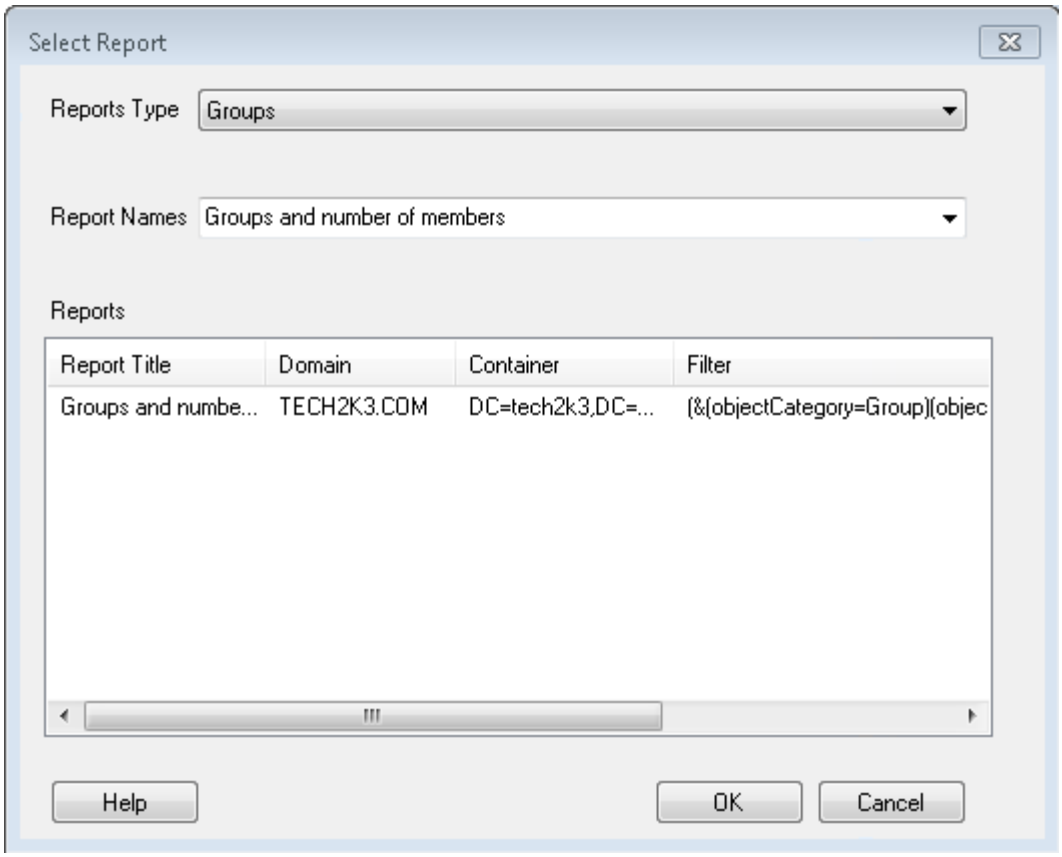


Figure - The Select Report dialog box

iv. Repeat the step 4(iii) to add more reports criteria for the job, if required.

5. Click the **Notification** tab and type the e-mail address of recipients in the **To** box to whom you want to send reports created by the job. For multiple addresses, use semicolons to separate each.

Part 6: Password Center

This part of the documentation covers the Password Center module of GroupID. The detailed information on how Password Center empowers network users to manage their user accounts is covered.

Chapter 21: Introduction, introduces you with the Password Center and its user interface.

Chapter 22: Setting Up a New Portal, provides information on creating a new portal and linking it with identity stores.

Chapter 23: Portal, covers how you can control the portal settings according to your requirements.

Chapter 21: Introduction

This chapter provides a brief overview of Password Center and its key features. The software and other requirements are also covered here. This chapter also helps you to get familiarized with Password Center user interfaces. The chapter is divided into following sections:

Password Center - Overview, provides a brief overview of Password Center.

Features, discusses the key features of Password Center.

Requirements for Password Center, includes the software requirements and other requirements for Password Center and includes instructions on setting them up.

Password Center User Interfaces, introduces you to the Password Center interfaces in the management console and the appearance of Web Portal for normal users and helpdesk users.

Password Center - Overview

With Password Center, take the concept of user empowerment one step further by enabling your network users to help themselves in performing tasks that were previously considered only doable by network administrators. Account lockout, password reset and change password are functions that your users can now perform on their own using a Web browser in a secure and safe manner.

Password Center empowers administrators by letting them control and customize the availability of these services. It also provides options that extend the default Active Directory password policy and allows you to further set specifications for password complexity.

Features

Delegating Password Management and Account Unlock Operations

In most organizations, the frequent requests that network administrators receive from users are regarding resetting their password or unlocking their accounts. Password Center reduces the daily workload of network administrators by delegating the account management tasks to users themselves. With Password Center, they can unlock their account, change and reset their password using a Web based interface in a secure and safe manner.

Added Password Validations

With Password Center, administrators can extend the password validation and complexity policy of an Active Directory domain to include more password validation rules according to your organizational needs. These rules are enforced on all users belonging to that domain attempting to change or reset their password using the Password Center Portal.

Second Way Authentication

Password Center primarily serves those network users who have enrolled their accounts on the portal. However; for the users who are not enrolled yet, Password Center provides the means to facilitate them by introducing a second way authentication method. Second Way Authentication (SWA) enables unenrolled users to authenticate themselves on a portal by answering questions that are based on their Active Directory profile.

Helpdesk

For those users who have forgotten their password or their account has been locked out and they are not even able to log on to the computer to use the Password Center Portal, helpdesk group is there to help them. Helpdesk group serves both enrolled and unenrolled users after authenticating them and can unlock their account or reset their password on request.

Requirements for Password Center

Password Center requires Microsoft Internet Information Server (IIS) 6.0 or higher for Portal creation. The IIS is Microsoft's implementation of a Web server for the Windows platform. IIS should be installed on the same machine where GroupID is installed.

Requirements for Helpdesk

The users whom you want to assign the helpdesk permissions should be the members of a local computer group on the machine where Password Center is installed. To create the group:

1. Click Windows Start button, click **Control Panel**, click **Administrative Tools** and then double-click **Computer Management**.
2. Expand **Local Users and Groups**.
3. Right-click **Groups** and click **New Group**.
4. On the **New Group** dialog box:
    i. In the **Group Name** box, type the name of the group.
    ii. In the **Description** box, type a brief description of the group.
    iii. Click **Add** to add members to the group.
    iv. Click **Create**.

You must be logged on as Administrator or as a member of the Administrators group to create a new group.

Password Center User Interfaces

Password Center provides two interfaces for users account management:

- Password Center Administrator
- Password Center Portal

Password Center Administrator

The Administrator interface - the **Password Center** node in the tree view of GroupID Management Console - enables administrators to monitor and control the overall configuration of identity stores and Password Center portals. Administrators can create new identity stores, manage security questions list that will be available to users while enrolling their accounts and changing or resetting passwords, apply additional password validation rules and configure notification settings. They can also create new portals and link identity stores with them to facilitate their users with the account management operations.

Password Center Portal

This is the interface that is available to the end users after the Administrator has created and configured the portal. The Web portal allows users to carry out certain tasks based on their roles.

Password Center in GroupID Management Console

In GroupID Management Console, **Password Center** node appears below **Automate**. From here, you can establish links with identity stores for facilitating users of that identity store with the account unlocking, password change and reset services. Expand the Password Center node to view its sub-nodes. The sub-nodes of Password Center allow you to control the configuration of your Password Center Portals and identity stores. Right-clicking a node at any level, including the Password Center node itself, will display the shortcut menu with commands that you can execute at that level.

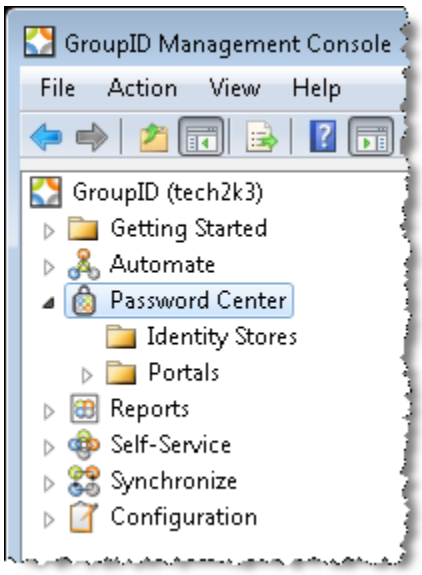


Figure - The Password Center node

Following is a summary of the Password Center sub-nodes:

Sub-node	Description
Identity Stores	Shows the list of **identity stores** and the list of security questions in the **global pool**. Each identity store has many configurations associated with it that control the identity store itself, the security questions at its local level, password validation rules and notification settings.
Portals	Shows the list of existing Password Center Portals. For each portal, there are configurations associated with it that controls the behavior of the portal. These settings are explained in detail in the **Chapter 23: Portal**.

Password Center Portal

Password Center Portal is further divided into two user interfaces:

- PCP for Users
- PCP for Helpdesk

PCP for Users

This is the user interface that is available to every network user belonging to an identity store configured for the portal and allows users to unlock their accounts, change and reset their passwords.

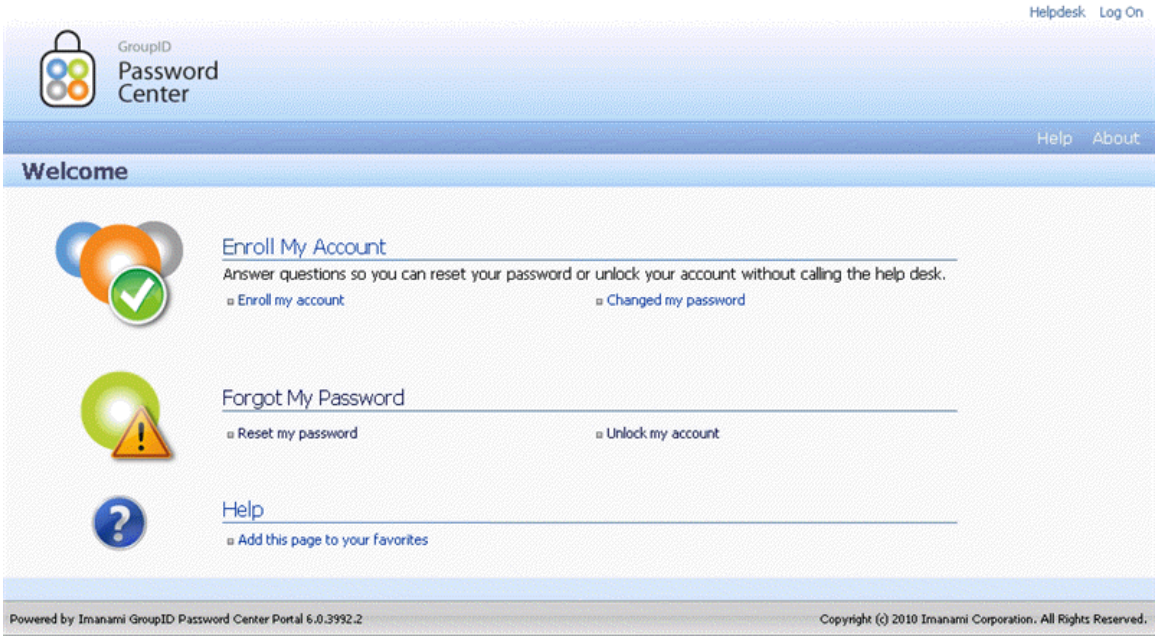

Helpdesk Log On
GroupID
Password Center
Help About
Welcome
Enroll My Account
Answer questions so you can reset your password or unlock your account without calling the help desk.
Enroll my account
Changed my password
Forgot My Password
Reset my password
Unlock my account
Help
Add this page to your favorites
Powered by Imanami GroupID Password Center Portal 6.0.3992.2
Copyright (c) 2010 Imanami Corporation. All Rights Reserved.

Figure - The Password Center Portal Interface for network users

PCP for Helpdesk

This interface is only available to the members of helpdesk group configured while creating the portal. For more information on configuring helpdesk group, see **Security Settings** in **Chapter 23: Portal**. A helpdesk user can reset passwords and unlock accounts of other users contacting them over phone.

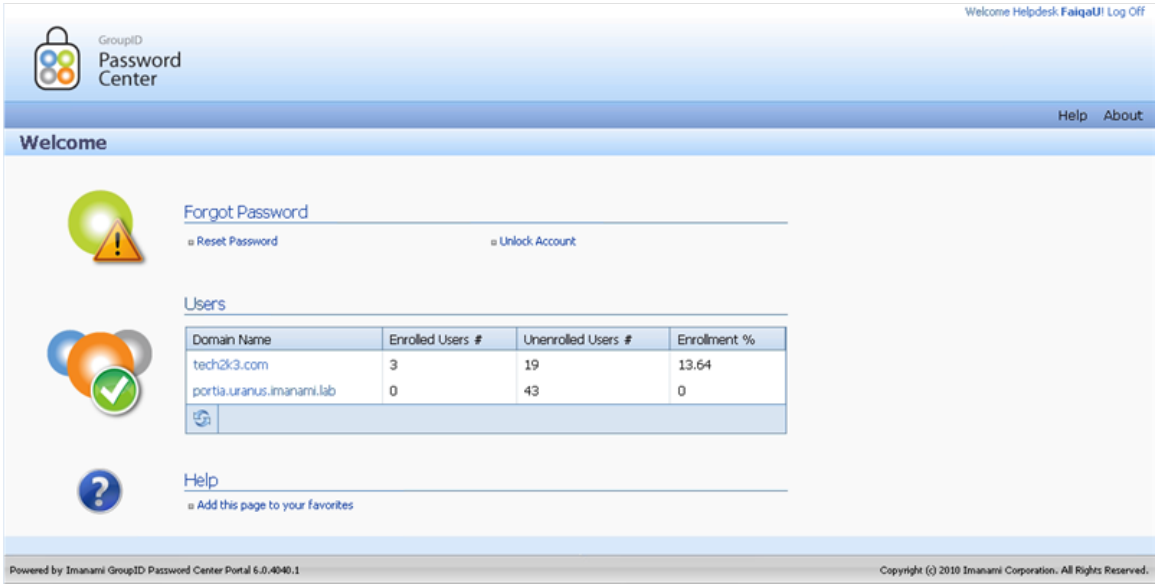


Figure - The Password Center Portal Interface for network users

Chapter 22: Setting Up a New Portal

This chapter covers the overall process of setting up a new Password Center Portal starting from the Identity Store creation to linking them with the portal and then setting up a helpdesk group.

This chapter is divided into the following sections:

Identity Stores, provides instructions on setting up a new identity store and customizing it according to your requirements.

Creating a New Portal, provides step by step information on creating a new portal.

Identity Stores

An Identity store is an Active Directory domain that is linked to a Password Center Portal for facilitating its users with the account unlocking, password change and reset services. Each identity store requires a service account that it uses to carry out the password related operations on the data store requested by the portal users. The service account should have sufficient privileges on the data store to carry out these tasks. Identity store also has its own security questions pool that it uses for authenticating users attempting to reset their password, or unlock their account. Password validation rules can also be enforced for the identity store according to your organizational policies.

Follow the instructions provided below to create a new identity store:

1. Launch GroupID Management Console.
2. Expand the **Password Center** node, right-click **Identity Stores** and then click **New Identity Store**.
   This will start the wizard for creating a new identity store.
3. On the welcome page of the wizard, read the welcome message and click **Next**.
4. On the **Identity Store Details** page, provide the following information:
   i. In the **Name** box, type the name of the identity store.
   ii. In the **Service Account** box, type the service account name on the identity store preceded by the identity store name and a backslash (\) which will be used by the Password Center Portal for unlocking accounts, resetting and changing passwords. The service account should have enough permissions on the identity store to perform the operations supported by the portal.
   iii. In the **Service Account Password** box, type the password of the given service account.
   iv. In the **Confirm Password** box, retype the service account password for confirmation.
   v. The **Enabled** check box is selected by default showing that this identity store will be available to be linked with any Password Center Portal, as created. You can clear this check box to create the identity store as disabled.
   vi. Click **Next**.

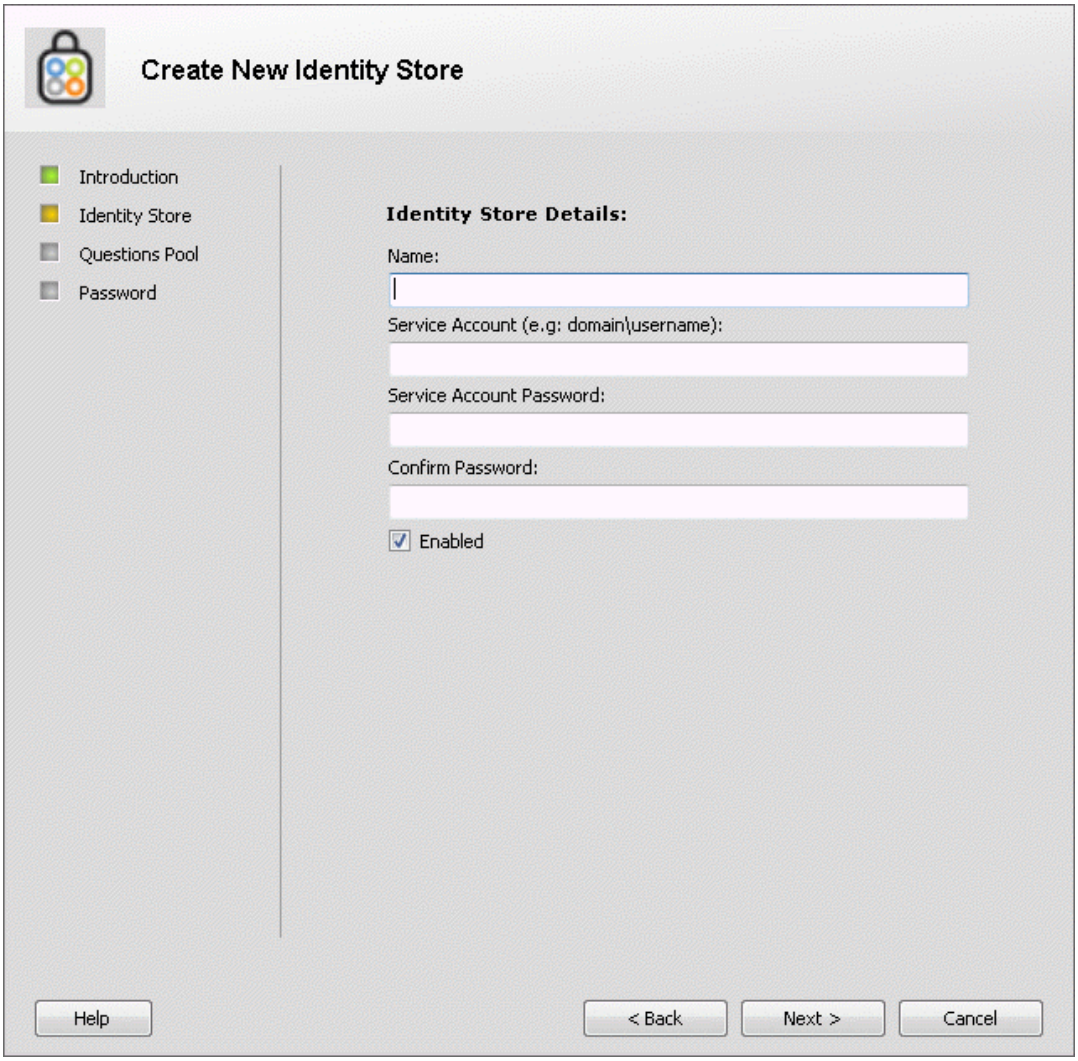


Figure - The Identity Store Details page

5. The **Security Questions** page shows the list of questions that are defined in the global security questions pool. You can select as many questions as required from the list or you can add more security questions that will be specific to this identity store.

    - **To select a security question**, click its check box.
    - **To add a new security question**, type the question in the **Security Questions** box and click **Add**.

6. Click **Next**.

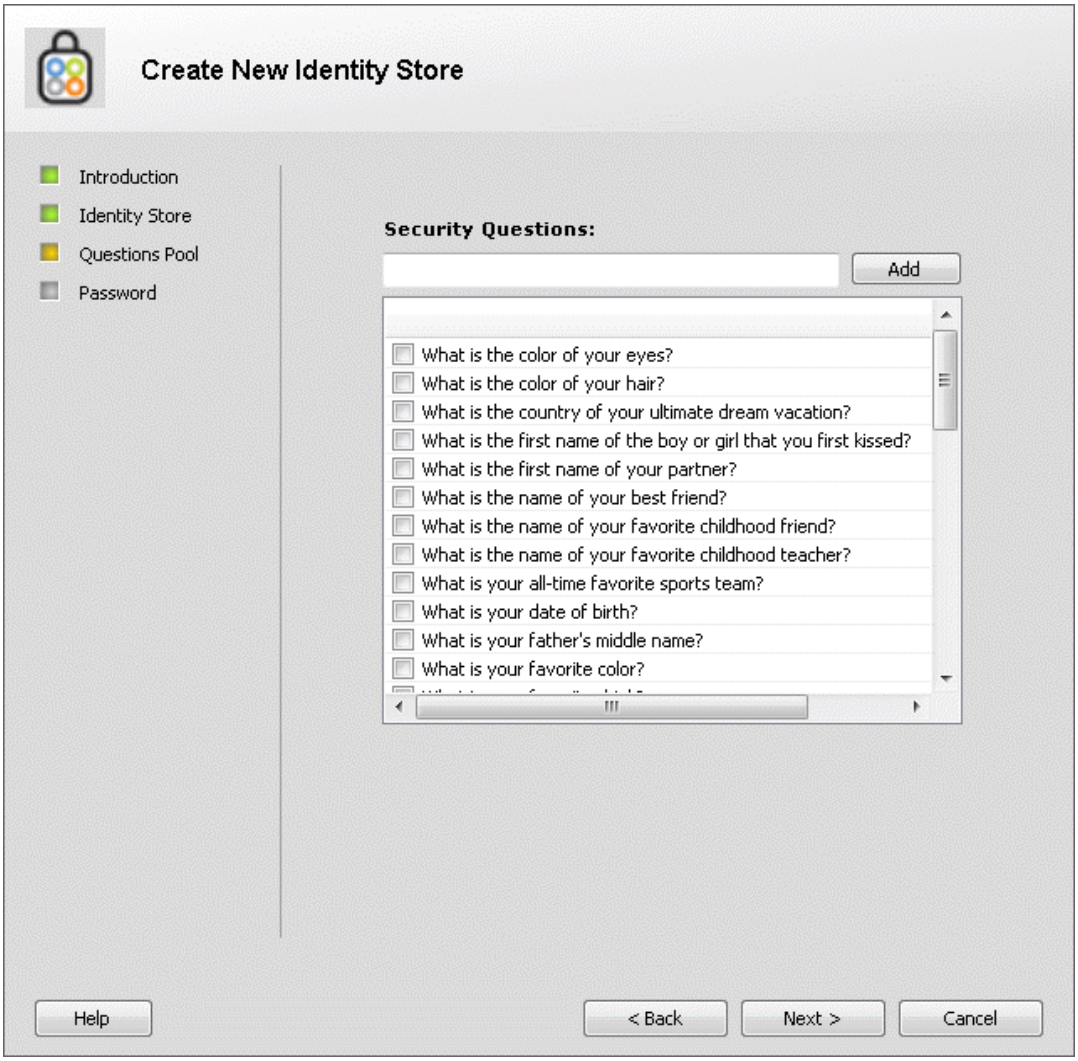

Create New Identity Store
Introduction
Identity Store
Questions Pool
Password
Security Questions:
Add
What is the color of your eyes?
What is the color of your hair?
What is the country of your ultimate dream vacation?
What is the first name of the boy or girl that you first kissed?
What is the first name of your partner?
What is the name of your best friend?
What is the name of your favorite childhood friend?
What is the name of your favorite childhood teacher?
What is your all-time favorite sports team?
What is your date of birth?
What is your father's middle name?
What is your favorite color?
Help
< Back
Next >
Cancel

Figure - The Security Questions page

7. On the **Password Validation** page, set the number of security questions to show on users' profile, the minimum answer length, account lockout settings on entering wrong answers, functions to be made available to the users and password validation checks.

8. Click **Finish**.

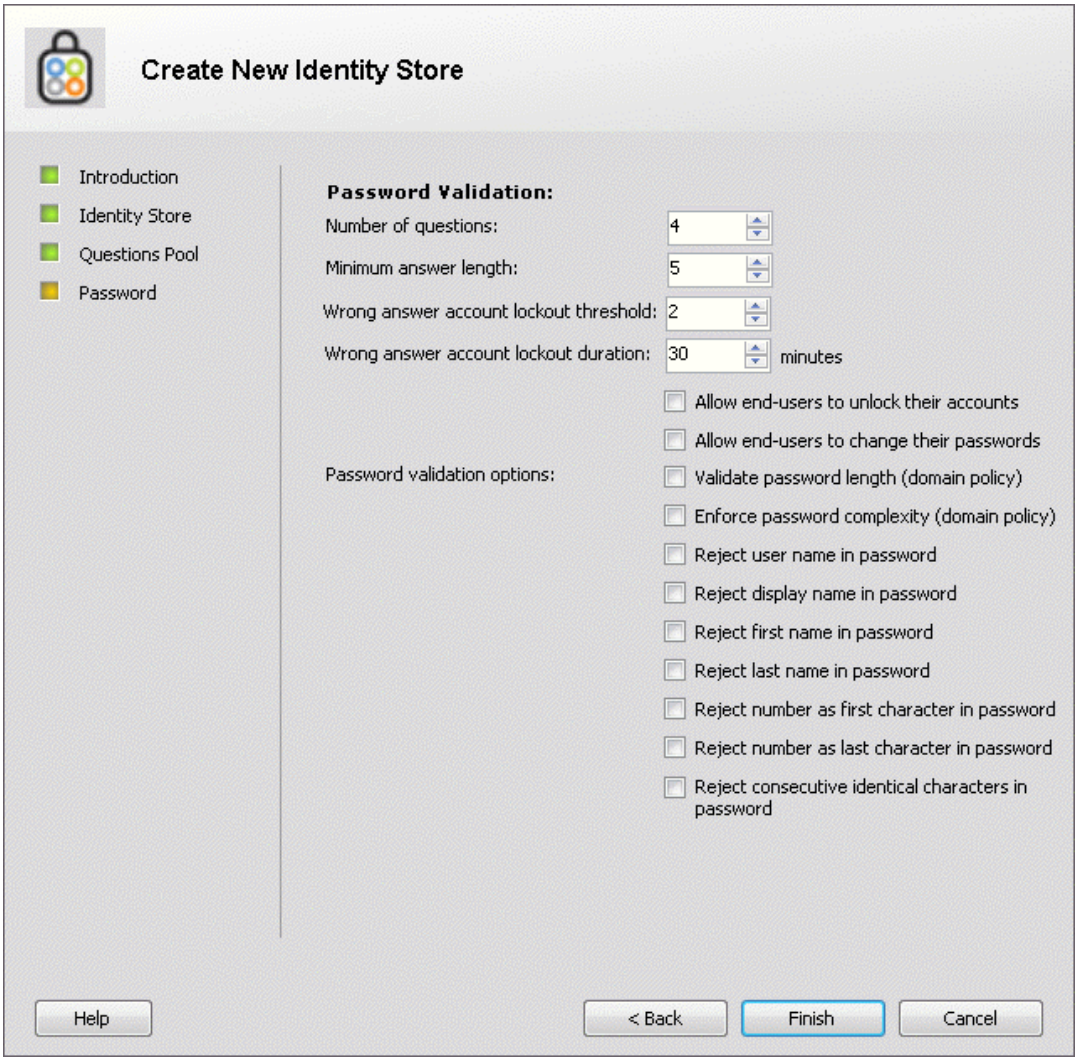


Figure - The Password Validation page

Security Questions

The purpose of security questions is to authenticate Password Center Portal users attempting to reset their password, or unlock their account. The security questions are used in creating the profiles of users who enroll for the Password Center Portal with which this identity store is associated and also to authenticate enrolled users when they perform certain operations using the Portal.

Security questions are divided into two pools:

- Global Pool
- Local Pool

Global Pool

Global pool of security questions is available out of the box for all identity stores when creating or modifying them. You can add more questions to this pool and delete existing ones. To add a new question to the global pool:

1. Expand the **Password Center** node, and then click **Identity Stores**.
2. Click the **Security Questions** tab.
3. In the box available above the questions list, type the security question.
4. Click **Add**.

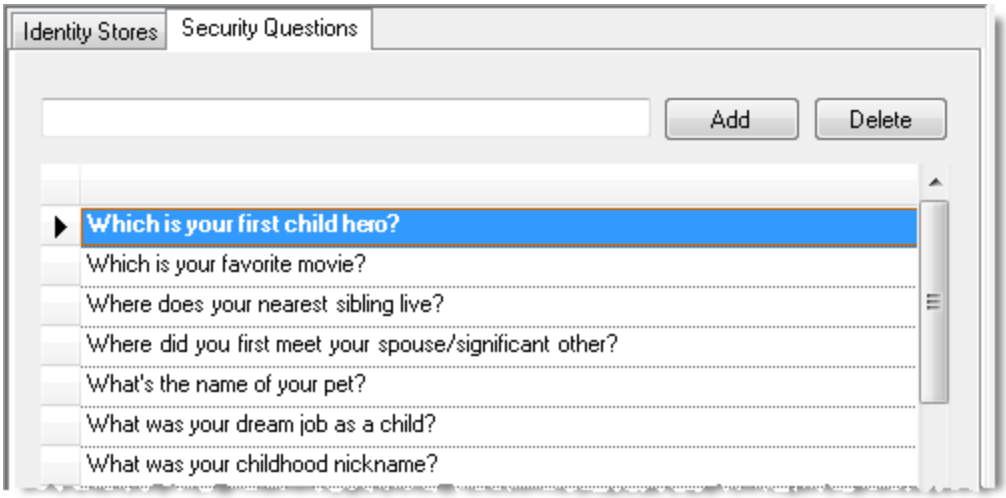

Identity Stores
Security Questions
Add
Delete
Which is your first child hero?
Which is your favorite movie?
Where does your nearest sibling live?
Where did you first meet your spouse/significant other?
What's the name of your pet?
What was your dream job as a child?
What was your childhood nickname?

Figure - The Security Questions tab showing the security questions in the global pool

To delete a question, select it from the list and click **Delete**.

Local Pool

In addition to global pool, a local pool of security questions is maintained individually for every identity store. The scope of the questions defined for this pool is limited to the identity store for which it is defined and cannot be shared with other identity stores. There are two ways to add questions to this pool:

1. **While creating the identity store**, for more information on adding questions while creating identity stores, see **Identity Stores**.
2. **Using identity store Properties dialog box**, the instructions below explain the process of adding questions:
    i. Expand the **Password Center** node, and then click **Identity Stores**.
    ii. On the **Identity Stores** tab, right-click the required identity store and click **Properties**.
    iii. Click the **Security Questions** tab.
    iv. Click **Add**.
    This displays the **New Question** dialog box, where:
        - In the **Questions** box, type the security question.
        - Click **OK**.

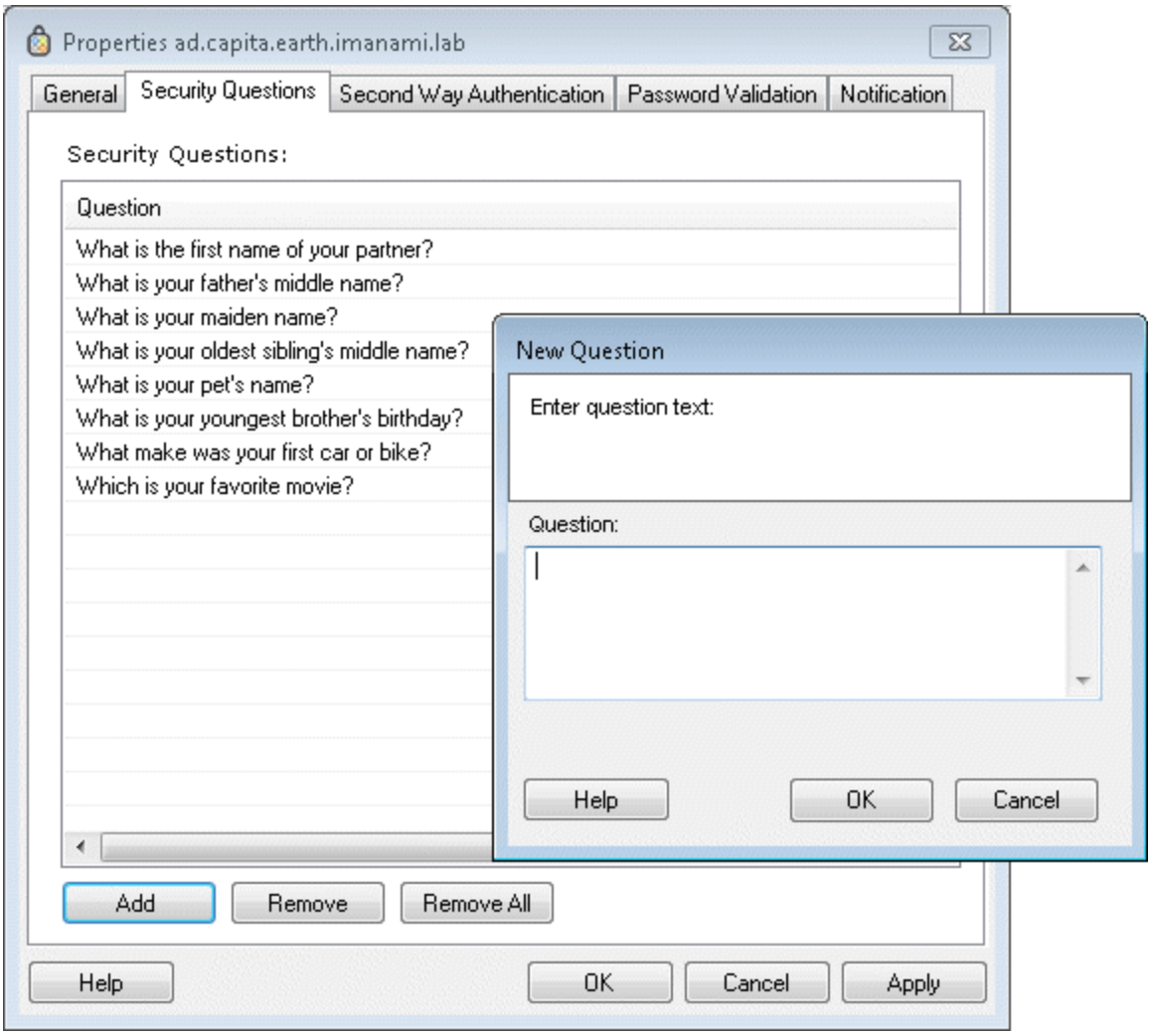


Figure - The New Question dialog box

You can click **Remove** to remove the selected question and click **Remove All** to clear the security questions list.

Second Way Authentication

This authentication method provides the means to facilitate users that have not had the opportunity to enroll their accounts on the Password Center Portal. Second Way Authentication (SWA) enables such users to authenticate themselves on a portal by answering questions that are based on their Active Directory profile.

When setting up SWA, the administrator specifies a set of security questions along with an Active Directory schema attribute for each of them. The answer provided by the user for a question is matched to the value of that attribute in Active Directory. If answers for all questions match the values for attributes in the directory, the authentication will be successful and the requested action will be carried out.

SWA is disabled by default when a new identity store is created. You have to enable it and add security questions for it.

To enable SWA:

1. Expand the **Password Center** node, and then click **Identity Stores**.
2. On the **Identity Stores** tab, double-click the required identity store.
   This opens the Properties dialog box for the selected identity store.
3. On the Properties dialog box, click the **Second Way Authentication Questions** tab.
4. Select the **Enable Second Way Authentication** check box.
5. Click **Apply**.

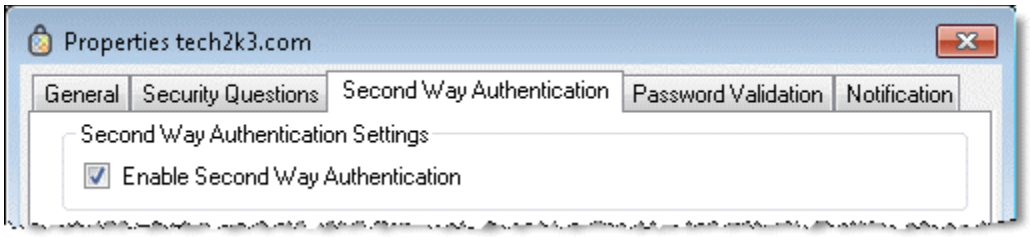


Figure - The Enable Second Way Authentication check box

To add a new security question for SWA:

1. On the **Second Way Authentication Questions** tab, click **Add**.
   This opens the **New Question** dialog box.
2. On the **New Question** dialog box:
   i. In the **Question** box, type your question.
   ii. In the **Schema Attribute** list, select the Active Directory schema attribute to map with this question.
   iii. Click **OK**.

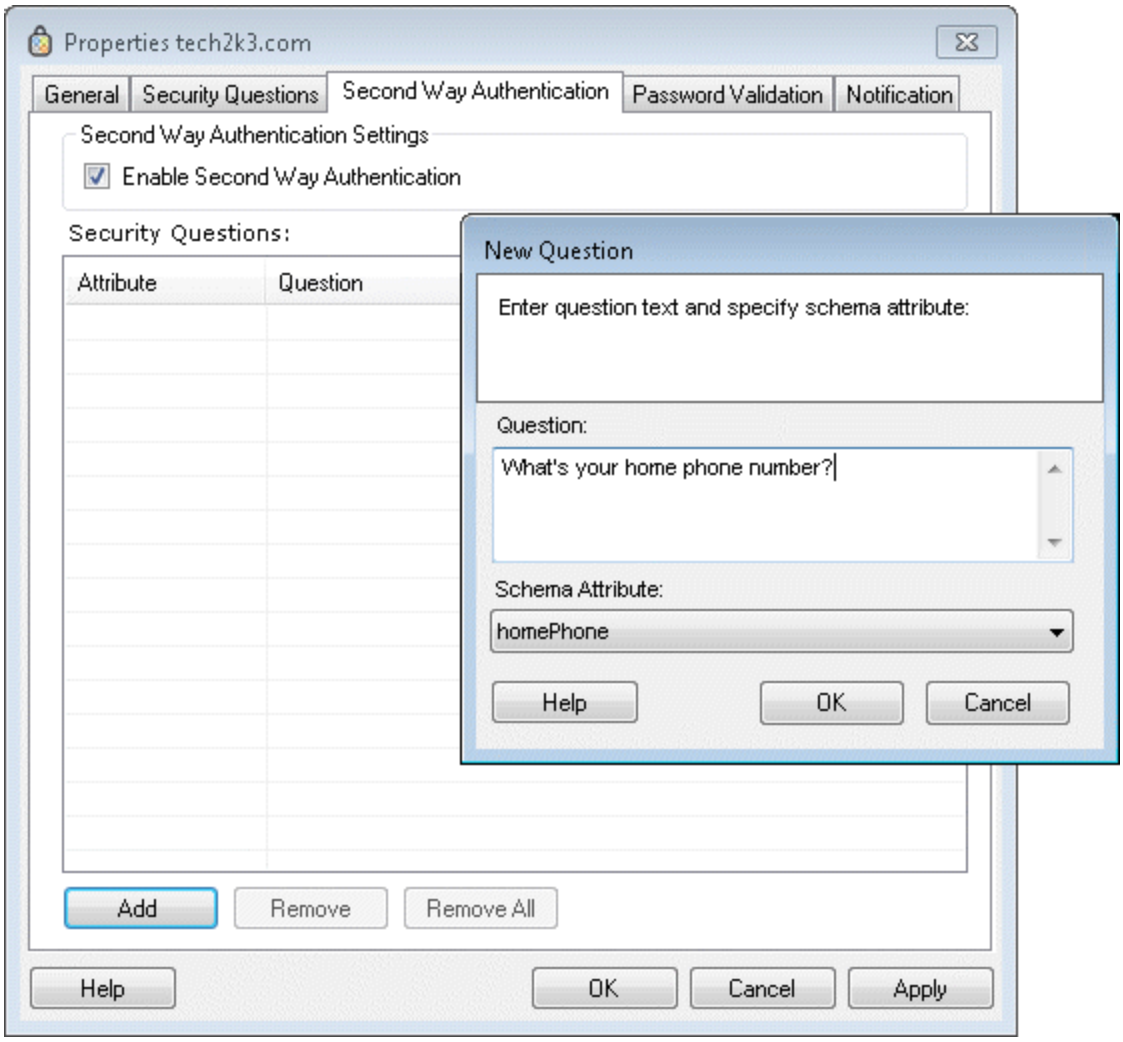


Figure - The New Question dialog box

Security Questions and Answers Settings

With Password Center, you can control the number of security questions to show the user while enrolling their account, minimum characters the user must enter for the answer of a security question and the account lockout policy on attempting wrong answers for a number of times. All these settings can be configured individually for each identity store using the **Password Validation** tab on the Identity Store **Properties** dialog box.

Below is the list of all related settings:

	Setting	Description
1.	Number of questions	The number of security questions to include in user profile. This setting will only be available if notifications are configured for the identity store. Changing the number of security questions for an existing identity store will require all its enrolled members to enroll again. On saving the changes, a notification e-mail will be automatically sent to all previously enrolled members asking them to re-

	Setting	Description
		enroll themselves using the portal.
2.	Minimum answer length	The minimum number of characters allowed in the security questions' answer. Users will not be able to save their answers if their characters are less than what is set here.
3.	Wrong answer account lockout threshold	The number of wrong attempts to answer a security question after which the user account's access to the portal will be locked out for the time specified in the **Wrong answer account lockout duration** box.
4.	Wrong answer account lockout duration	The number of minutes for which the user account's access on the portal will remain locked out if the user enters wrong answer for a security question for the number of times set in the **Wrong answer account lockout threshold** box.

Password Validations

Each Active Directory domain has a password validation and complexity policy associated with it. All users belonging to that domain have to follow the password policy while setting their passwords. With Password Center, you can extend this policy further and set your own specifications for password validation and complexity according to your organizational needs.

The list below contains the description of each setting:

	Setting	Description
1.	Allow end-users to unlock their accounts	Enables your network users to unlock their accounts using the Password Center Portal.
2.	Allow end-users to change their passwords	Enables your users to change their passwords using the Password Center Portal.
3.	Validate password length (domain policy)	Validates the domain password length policy on the Portal. This option works only if the password policy is enforced in your Active Directory domain. Selecting or clearing this setting does not change the Active Directory domain policy. It only determines if the policy should be validated along with the other options selected on this page.
4.	Enforce password complexity (domain policy)	Validates the domain password complexity policy on the Portal. This option works only if the password policy is enforced in your Active Directory domain. Selecting or clearing this setting does not change the Active Directory domain policy. It only determines if the policy should be validated along with the other

	Setting	Description
		options selected on this page.
5.	Reject user name in password	Prevents passwords that contain user's account name.
6.	Reject display name in password	Prevents passwords that contain user's display name.
7.	Reject first name in password	Prevents passwords that contain user's first name.
8.	Reject last name in password	Prevents passwords that contain user's last name.
9.	Reject number as first character in password	Prevents passwords starting with a number.
10.	Reject number as last character in password	Prevents passwords ending with a number.
11.	Reject consecutive identical characters in password	Prevents the consecutive use of identical characters in passwords.

There are two ways to set the password validation rules for an identity store:

1. **While creating the identity store**, for more information on setting password validations while creating identity stores, see **Identity Stores**.
2. **Using identity store Properties dialog box**, the instructions below explain the process:
    i. Expand the **Password Center** node, and then click **Identity Stores**.
    ii. On the **Identity Stores** tab, right-click the required identity store and click **Properties**.
    iii. Click the **Password Validation** tab.
    iv. Select the check box of the required option to apply the setting and clear its check box to cancel the setting.

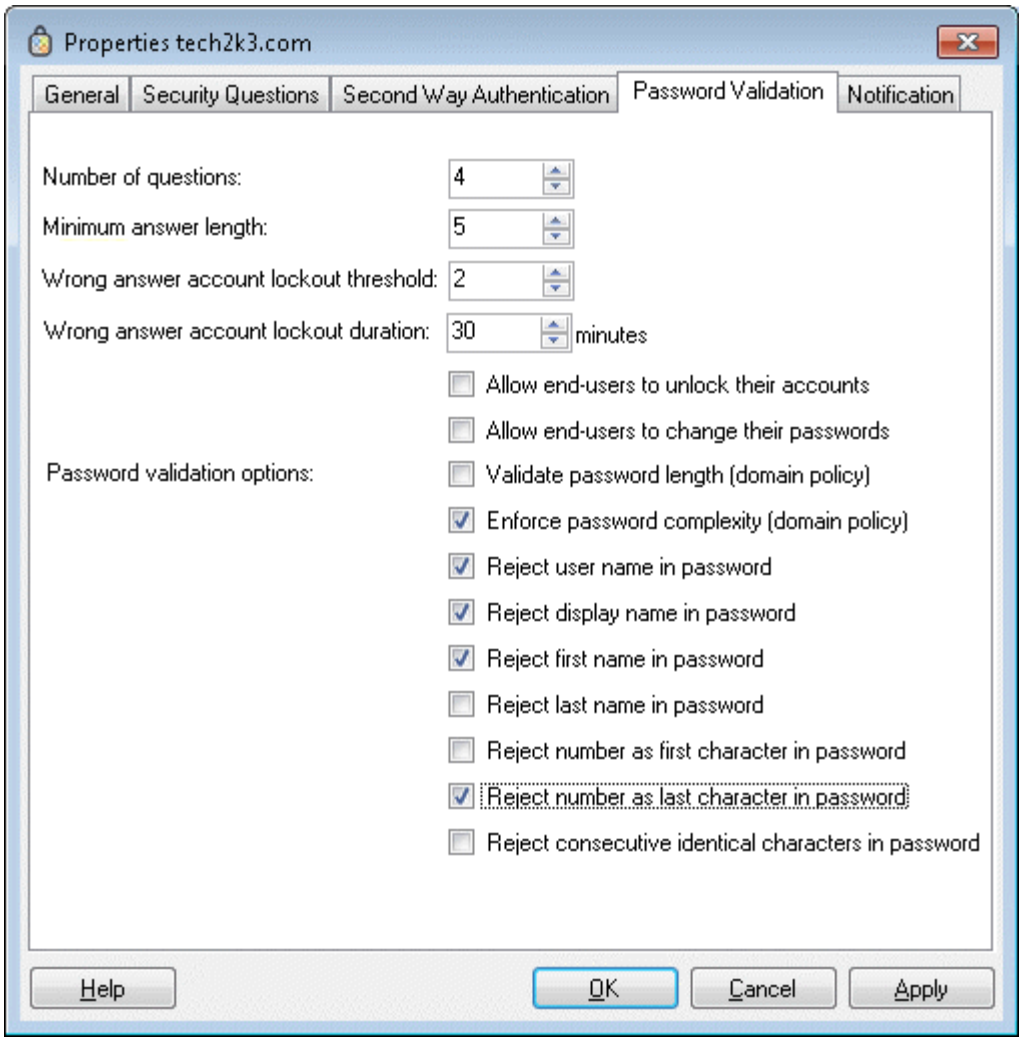


Figure - The Password Validation tab on the Identity Store Properties dialog box

Notifications

Password Center Portal can send notifications about actions performed by users belonging to an identity store through the portal. It can even notify end users carrying out the password management tasks. Helpdesk users can send reminder notifications to the users who have not yet enrolled their accounts using the portal. These notifications contain URLs that redirect them to pages of the portal from where the required actions can be carried out.

By default, notifications are not configured for an identity store. For such identity stores, an information message will also appear on top of the identity store's properties dialog box informing you that its notification settings are not configured.

Sending notifications requires the SMTP server to be configured for the identity store. You also need to specify the e-mail addresses to which you want to send the notifications.

The steps below guide you on how to configure notifications for an identity store:

1. Under the **Password Center** node, click **Identity Stores**.
2. On the **Identity Stores** tab, right-click the required identity store and click **Properties**.

3. Click the **Notification** tab.

    i. In the **Notification method** list, click **SMTP**. This enables the fields in the **SMTP Server Options** area.

    ii. In the **Server name/IP address box**, type the IP address or DNS name of the SMTP server to use for sending notifications. This server must allow relaying.

    iii. In the **Port** box, type the SMTP port to use when connecting. The default port is 25.

    iv. In the **From e-mail address** box, type the e-mail address to use as the sending address for notifications.

    v. In the **To e-mail address** box, type the recipient e-mail address or addresses (separated by semicolon (;)).

    vi. In the **CC e-mail address** box, type the e-mail address or addresses (separated by semicolon (;)) of the recipients who should receive a copy, if required.

    vii. You can select the **Notify end-user on enroll, unlock, change password and password reset** check box to have the end user notified along with the other recipients specified in the **To e-mail address** box.

    viii. In the **Password Center Portal URL** box, type the URL of any portal created for the Identity Store. This URL is used in the links given in e-mail notifications to direct the receivers to different pages of the portal depending on the action that they need to perform.

    ix. Click **OK**.

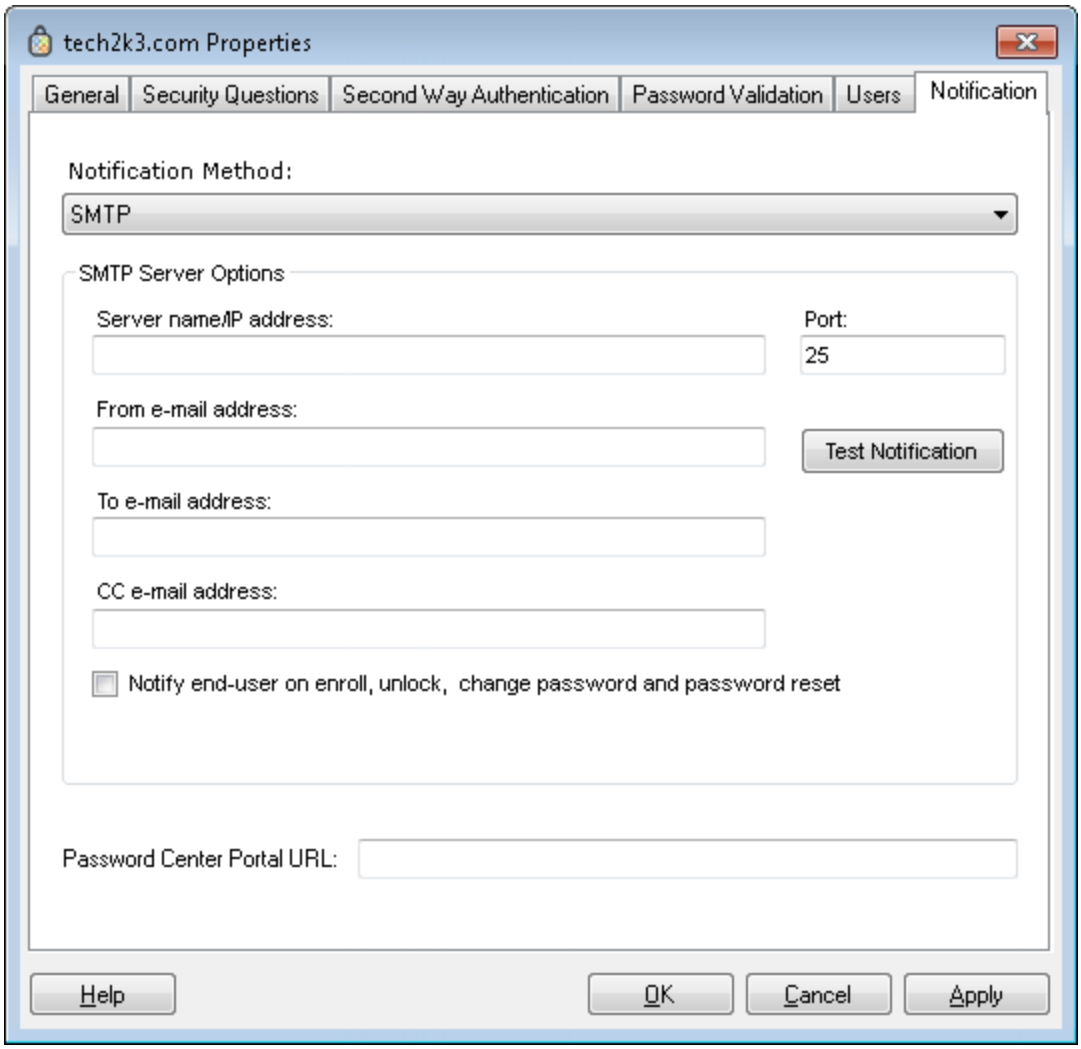


Figure - The Notification tab on the Identity Store Properties dialog box

Creating a New Portal

To provide password management capabilities to end-users, you first need to setup a new portal and link it with one or multiple identity stores. The users of these identity stores will be able to avail the account unlock, password change and reset services of the portal using a Web browser program.

Follow the instructions provided below to create a new Password Center Portal:

1. Launch GroupID Management Console.
2. Expand the **Password Center** node, right-click **Portals** and then click **Create**. GroupID displays the **GroupID - Password Center** dialog box.
3. In the **Server name** box, type the name of your portal or leave the default name and click **OK**. This will start the wizard for creating a new portal.

Figure - The GroupID - Password Center dialog box

4. On the welcome page of the wizard, read the welcome message and click **Next**.
5. On the **Identity Stores** page, select one or more identity stores from the **Identity Stores** list. To select an identity store, click on it once and to deselect it, click on it again.
6. Click **Next**.

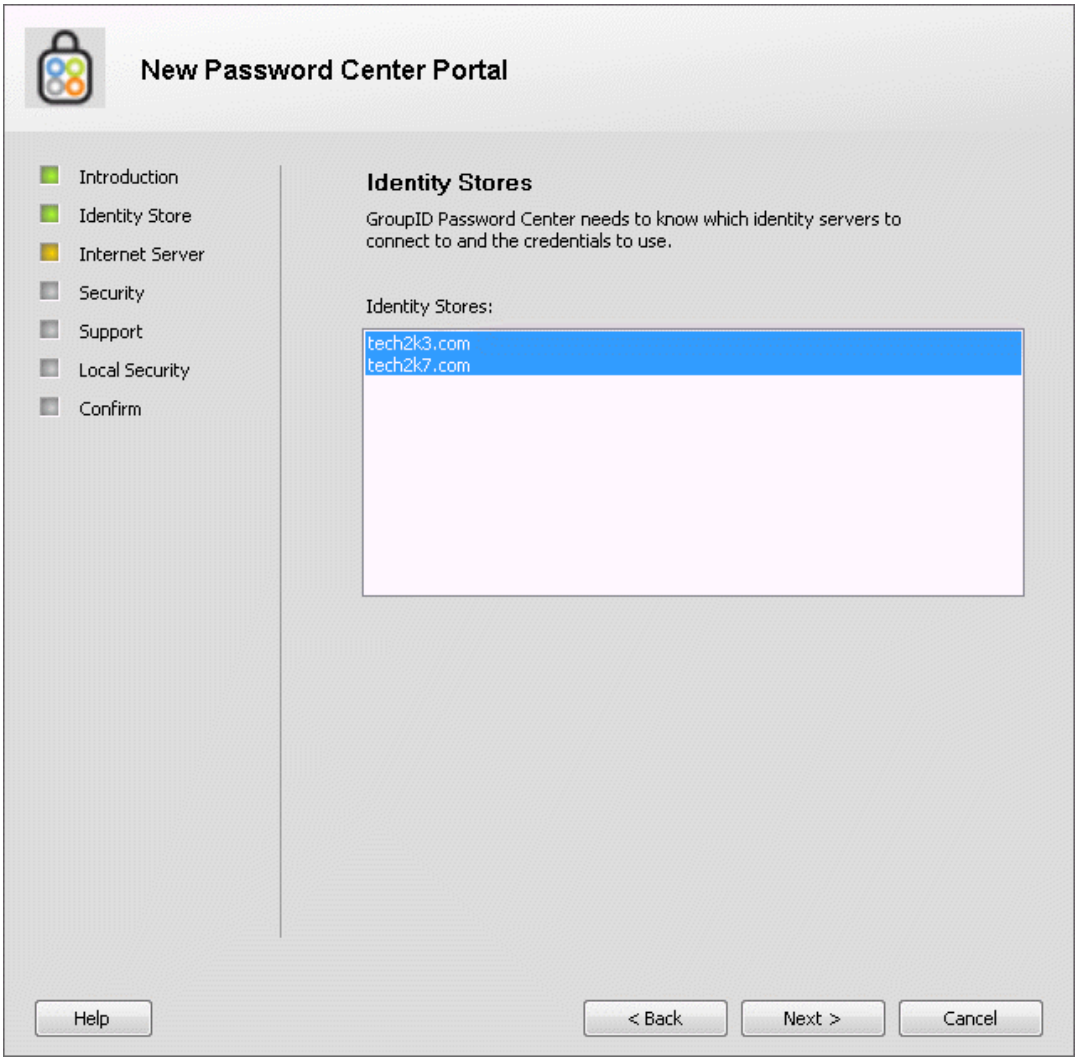


Figure - The Identity Stores page

7. On the **Internet Server** page, you make settings for the IIS virtual directory that will host the portal files. On this page:

    i. The **Path to Portal files** displays the physical path to the Portal's folder.

    ii. From the **IIS Server** list, select IIS site in which to host your Portal. **Default Web Site** is the default selection.

    iii. From the **Select default language** list, select your default language. The default selection for this is **English**.

8. Click **Next**.

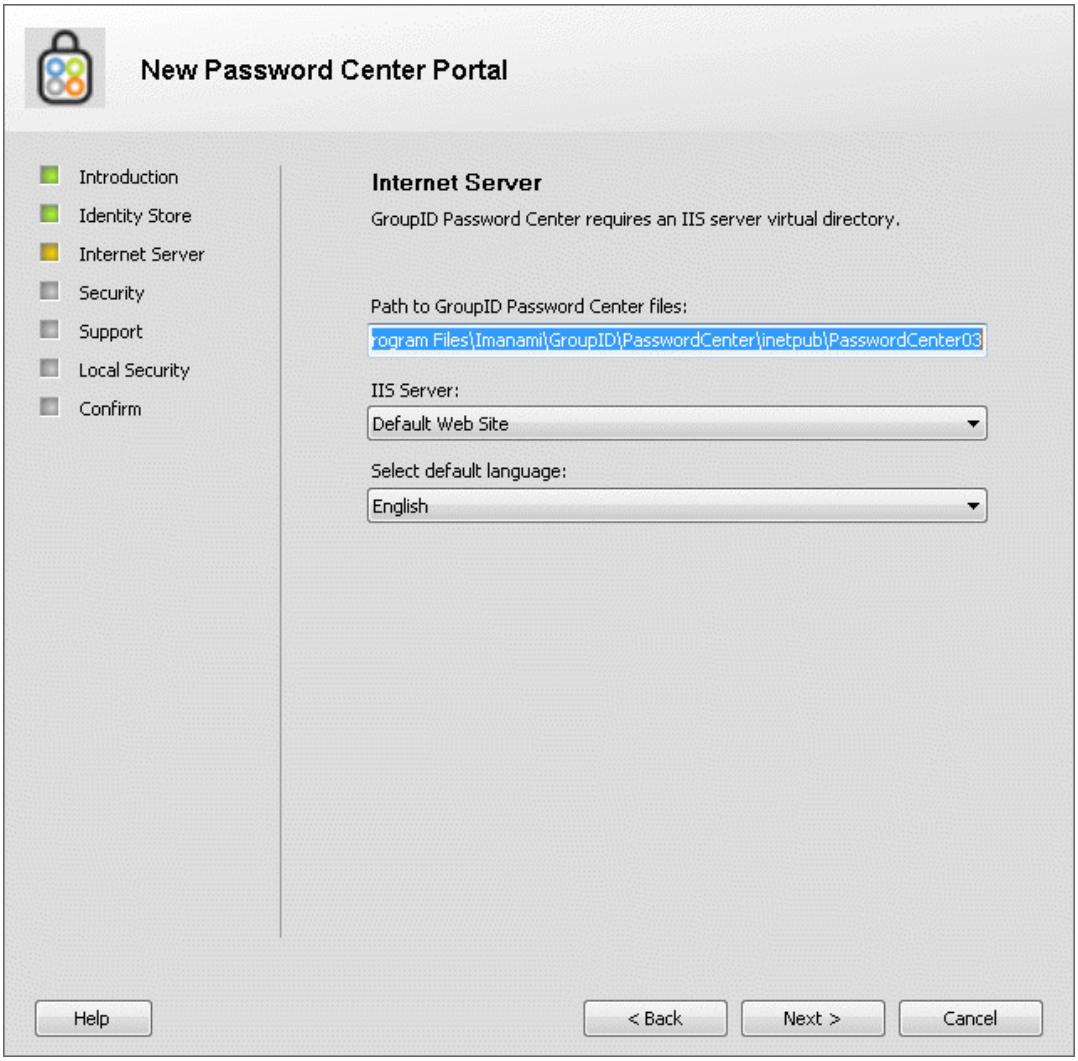


Figure - The Internet Server page

9. On the **Security** page, you specify the group that you want to assign the special helpdesk permissions. Helpdesk permissions enable the group members to perform password related operations and unlock computers on users' request. To set a **HelpDesk Group**:

    - Click the ... button.
    - On the **Select Local Group** dialog box, select the required group from the list and click **OK**.

10. Click **Next**.

Figure - The Security page

11. On the **Support Information** page, type the information for users of this portal to report their problems to the internal helpdesk or support team within your company:

    i. In the **Support group/administrator's e-mail address** box, type the e-mail address for the group or contact that will be responsible for providing support for this portal.

    ii. In the **Help URL** box, you can type the Internet address for a Web page or Web site where your portal users can find support material or report their problems.

12. Click **Next**.

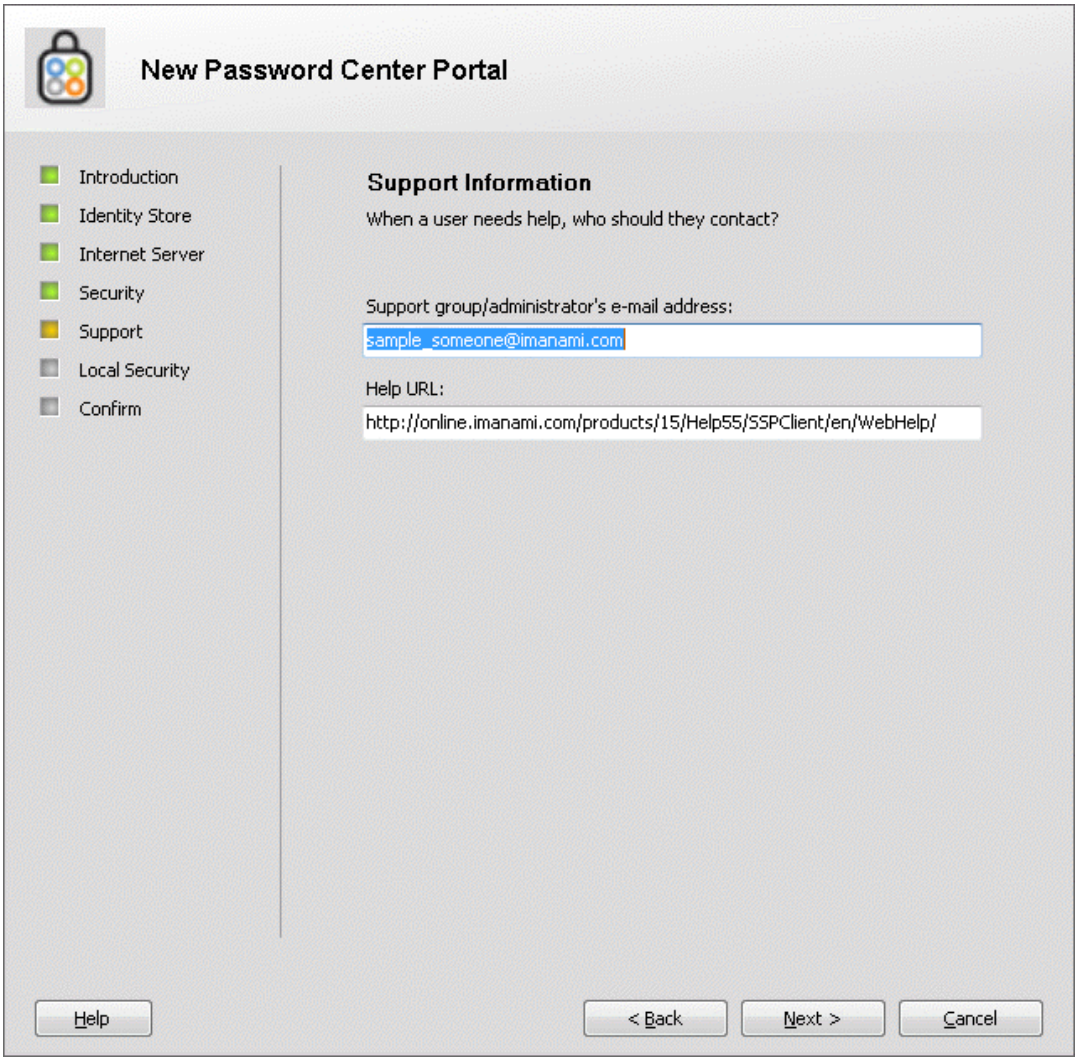


Figure - The Support Information page

13. The **Local Policy** page is for informational purposes only. Click the **Next** button after reviewing the information on the page and click **Next** to continue.

14. The **Confirm** page shows the information that you have entered on the previous pages. Verify the information on this page. If you need to change anything, click **Back** until you reach the required page.

15. After reviewing the information, click **Finish**. This step completes the setting up of a new portal. The portal is now available for access to your users using a Web browser.

Chapter 23: Portal Settings

This section provides information on controlling the overall configurations of the Portal. The configurations are divided into the following sections:

General Settings, explains how to change the display name of the portal.

Identity Store Settings, describes how to manage identity store links with the portal.

IIS, explains the IIS and default language settings for the Portal.

Security Settings, provides information on setting up a helpdesk group for the portal.

Support Settings, describes how you can modify the contact information for your internal support and the address of the online help.

Miscellaneous Settings, describes how to change the GroupID data service URL for portals.

General Settings

The display name of the portal that appears in the URL for accessing the portal, can be changed any time after its creation. However, changing the display name only changes its alias in IIS and does not rename its root folder.

To change the portal's display name:

1. Under the **Password Center** node, expand the **Portals** node.
2. Click the required portal's node, and then click the **General** tab.
3. In the **Virtual server display name** box, type the new name of the portal.
4. On the toolbar, click **Save** .

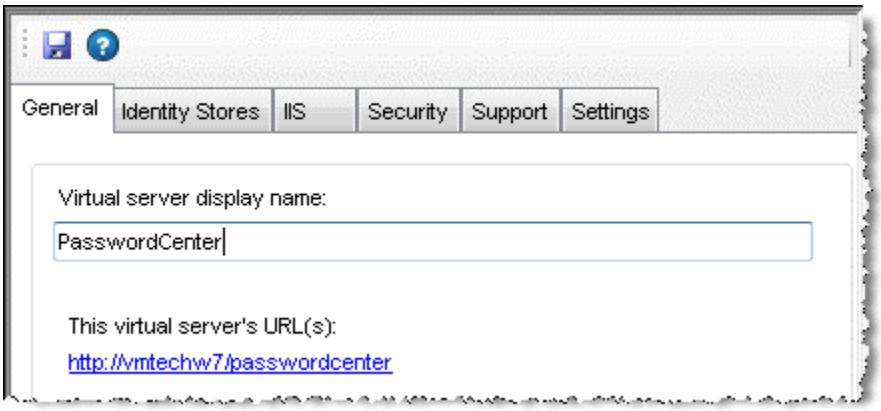


Figure - The General tab

Identity Store Settings

When you setup a new portal, you link identity stores with it to provide their users access to the portal. More identity stores can be linked to the portal and existing can be removed using the **Identity Stores** tab available on the portal's **Server** node.

To link more identity stores to the portal:

1. Under the **Password Center** node, expand the **Portals** node.
2. Click the required portal's node, and then click the **Identity Stores** tab.
3. Click **Modify**.
   This displays the **Edit Identity Stores** dialog box, where:
   i. From the **Non Selected Identity Stores** list, select one or more identity stores that you want to add. To select an identity store, click on it once and to deselect it, click on it again.
   ii. Click > .
   iii. Click **OK** to close the dialog box.

You can remove an existing identity store link by selecting it from the **Selected Identity Stores** list and clicking .

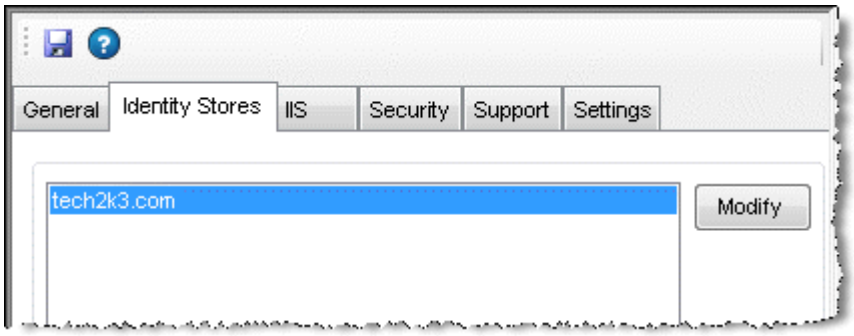


Figure - The Identity Stores tab

IIS Settings

Password Center Portal is deployed as an application on Internet Information Server (IIS). It also creates certain files on your local file system for operating that it copies from the templates directory to the specified path, when the portal is created. The physical path cannot be changed after the portal creation; however, you can change the IIS site for the Portal's application.

You can also change the default language for the Web browser of the user. Self-Service Portal detects the languages supported by the Web browser program of the user when they log on and attempts to load the interface with the correct language. If it does not support the language set for a user's browser, or it cannot detect the language settings of the Web browser, it will load this default language.

To manage the IIS settings, please follow the instructions given below:

1. Under the **Password Center** node, expand the **Portals** node.
2. Click the required portal's node, and then click the **IIS** tab.

To change the IIS site

1. From the **IIS Server** list, select the IIS site where you want to move the virtual directory of the portal.
2. On the toolbar, click **Save** .

To change the default language

- From the **Select default locality** list, click the required language.
- On the toolbar, click **Save** .

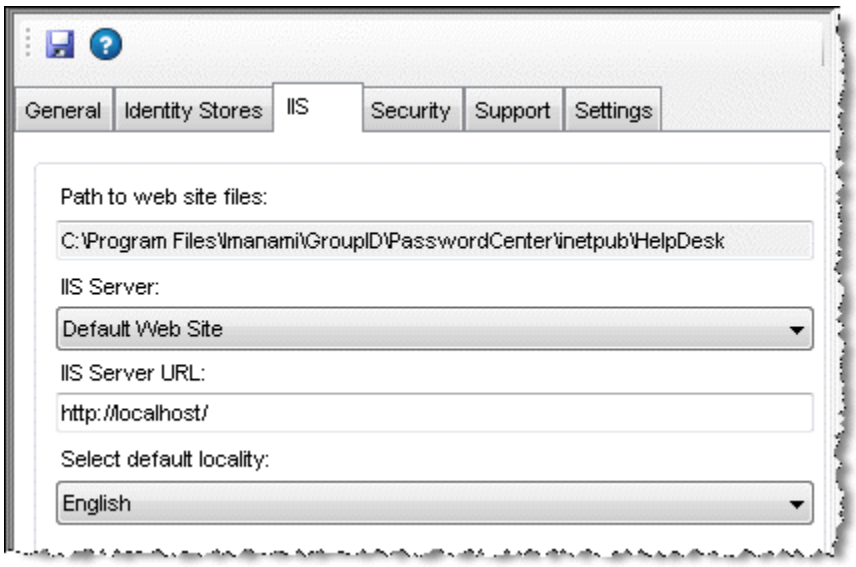


Figure - The IIS tab

Security Settings

Users visiting a Password Center Portal are authenticated by IIS. The types of authentication methods that you can configure for your Portal depend on the version of IIS installed on your server. IIS 6.0 supports eight authentication methods.

1. Anonymous authentication
2. Basic authentication
3. Digest authentication
4. Advanced Digest authentication
5. Integrated Windows authentication
6. UNC authentication
7. .NET Passport authentication
8. Certificate authentication

For more information about IIS authentication types, please refer to the Microsoft TechNet Web site - http://www.microsoft.com/technet.

The Helpdesk group

Password Center enables you to designate a local group that you want to assign special helpdesk permissions. The helpdesk concept is to facilitate IT support teams that serve users within an organizational setup. Helpdesk permissions enable members of such teams to perform password related operations and unlock accounts on users' request.

To set a helpdesk group:

1. Under the **Password Center** node, expand the **Portals** node.

2. Click the required portal's node, and then click the **Security** tab.
3. Click the ... button.
4. On the **Select Local Group** dialog box, select the required group from the list and click **OK**.
5. On the toolbar, click **Save**.

Figure - The Security tab

Support Settings

These settings determine how the users of your Web Portal can obtain support and help. You can set an e-mail address and a Web site link for this purpose. The e-mail will be available to the users on clicking the **Contact** link in the portal while the Web site address is mapped to the **Help** link. On clicking the Help link, the specified Web site will be opened up in a new browser window.

Also available on this tab are the log settings. The log settings here are specific to the portal under consideration and will take precedence over the global log settings. The global log settings apply to the whole Password Center module and are used as the default settings for new portals. The global log settings can be set from the GroupID Configurations dialog box.

Logging can be used for tracking events that might help in tracing out the cause of a problem. Usually they are used for debugging errors. Log settings and their configurations for Password Center are explained in the topic **Log Settings** in **Part 7: GroupID Configurations.**

To manage these setting, follow the instructions given below:

1. Under the **Password Center** node, expand the **Portals** node.
2. Click the required portal's node, and then click the **Support** tab.
   The tab, by default, shows the support contact, help and logging settings defined on the GroupID **Configurations** dialog box. These settings are explained in detail in the topic **Log Settings** in **Part 7: GroupID Configurations**. You can customize these settings individually for each portal.

To add an e-mail address

The e-mail address can be of a helpdesk user, contact or group.

1. In the **Support group/administrator's e-mail address** box, type the e-mail address.
2. On the toolbar, click **Save**.

To add a Web site address

The default URL set here points to Imanami's online help for Password Center portals . You can change this to point to your own version of the help, an internal helpdesk Web site, or similar.

1. In the **Help URL** box, type the Web site address.
2. On the toolbar, click **Save** .

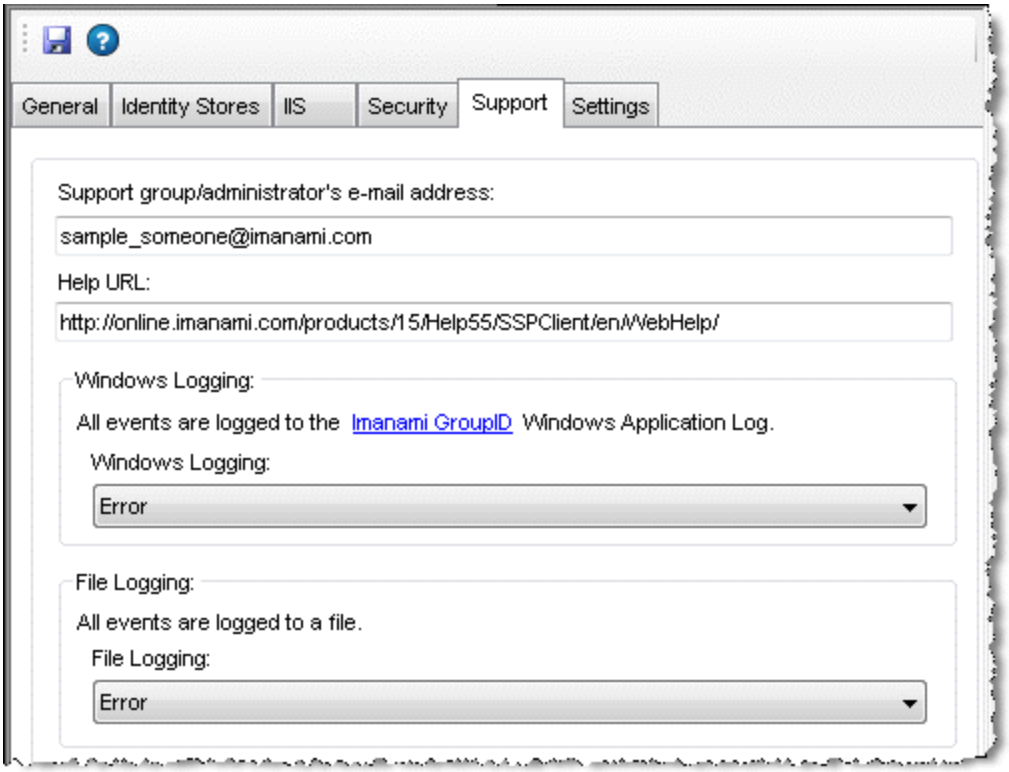


Figure - The Support tab

Miscellaneous Settings

The miscellaneous settings include only the GroupID Data Service URL setting for now. This is the individual setting for each portal and is not related to the global setting that is set in the Database settings provided on the **Configuration** dialog box.

When a new portal is created, the data service URL for it is copied from the global setting on the Configuration dialog box. However, if the data service URL for this global setting is changed at a later time, the new URL will not be updated for any of the existing portals. For all such portals you will have to manually update the data service URL using their individual setting.

To change the data service URL:

1. Under the **Password Center** node, expand the **Portals** node.
2. Click the required portal's node, and then click the **Settings** tab.
3. In the **GroupID Service URL** box, type the new data service URL.

4. On the toolbar, click **Save** .

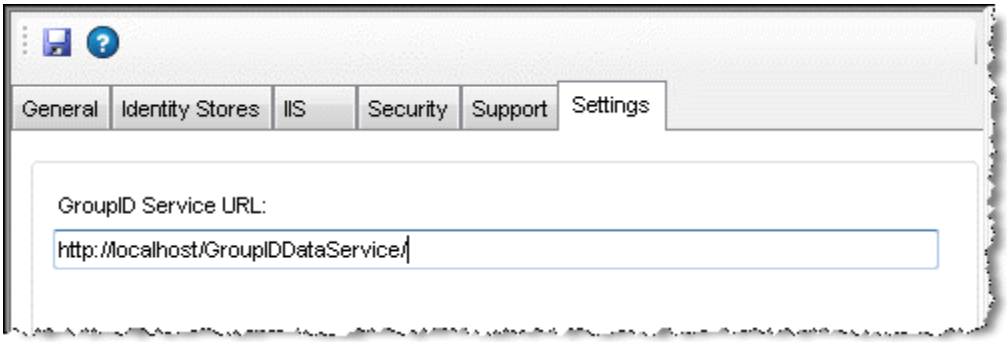


Figure - The Settings tab

Part 7: GroupID Configurations

This part of documentation explains certain global configurations that apply to multiple modules of GroupID. You will learn about the logging types supported in GroupID and the levels that determine detail to include in them. It also provides instructions for setting up a SMTP server that will be used by the modules for sending e-mail notifications. You will also learn how prefixes help you to maintain the naming consistency for groups. It also explains how you can configure GroupID Data Service and SQL Server database for storing GroupID configurations and other information. This part is divided into the following sections:

Log Settings, explains the logging types in detail and provides instructions on configuring them for GroupID modules.

Notifications Settings, provides instructions on configuring SMTP server for sending e-mail notifications.

Group, describes the purpose of Group Name Prefixes and provides instructions on configuring them.

Database and the Data Service Settings, provides instructions on configuring GroupID Data Service and SQL Server database.

History Settings, provides instructions on configuring actions for tracking their history.

Exchange, contains instructions on selecting the Exchange version for creating mail-enabled objects in a multi-Exchange environment.

Log Settings

GroupID enables you to log events for all modules that helps in crisis to identify the cause and rectifying it. GroupID supports two types of event logging: Windows Logging and File Logging.

Windows Logging

Windows Logging records events from all GroupID modules in a centralized event log named **Imanami GroupID** that can be viewed from the Windows **Event Viewer**. Windows logging divides events into five different levels depending on the type of information they log. Every successive event level incorporates the events of its preceding levels too. Below is the list of levels provided by Windows Logging.

	Level	Description
1.	Error	This is the default event level for Windows Logging. This level logs problems such as loss of data or loss of functionality.
2.	Warning	This level logs event that is not necessarily significant, but may indicate a possible future problem.
3.	Information	Setting this level logs events that describe the successful operation of a module or functionality.
4.	Success Audit	Setting this level logs events that record an audited security access attempt that is successful.
5.	Failure Audit	Setting this level logs event that records an audited security access attempt that fails.

File Logging

File logging records events for GroupID modules in log files saved on the file system. The location of these log files varies for Self-Service, Password Center and the rest of modules. For Self-Service and Password Center, the log files are created in a subfolder within the root directory of each Portal, that is ***X***:\Program Files\Imanami\GroupID*Module-Name*\Inetpub*Portal Name*\log (where ***X*** represents the installation drive). For Synchronize, Automate and Reports; the log files are stored in the temporary folder for the logged-on user which can be accessed using the **%TEMP%** environment variable. However; for scheduled jobs, the log files for these modules are created at, ***X***:\Windows\Temp (where ***X*** represents the Windows installation drive). This is because scheduled jobs are run under the local System account.

File logging uses the **Rollover Logging** mechanism to log events. This mechanism involves logging events in a text file. For the Self-Service Portal, the file is named as **GroupID6-SSP**; for Password Center Portal, the file is named as **GroupID6-PasswordCenter**; and for the rest of modules, the file has the name **~GroupID6**. When the size of a file reaches 100MB, a rollover occurs that archives the log file in the same directory by replacing its file extension with **.Log.*X*** (here ***X*** is a number from 1 to 10 representing the archiving order. The lower the number, the recent is the file). A new log file is created for maintaining the logs (with the name **GroupID6-SSP** for Self-Service Portal, **GroupID6-PasswordCenter** for Password Center Portal and **~GroupID6** for the rest of modules).

File logging divides events into six different levels depending on the type of information they log. Every successive event level incorporates the events of its preceding levels too. Below is the list of levels provided by File Logging.

	Level	Description
1.	All	This is the highest level of logging and logs every possible event in the log file.
2.	Debug	Setting the debug level designates fine-grained informational events that are most useful to debug the application.
3.	Info	Setting this level logs events that describe the successful operation of a module or functionality.
4.	Warn	Setting this level logs event that is not necessarily significant, but may indicate a possible future problem.
5.	Error	This is the default event level for file logging. Setting this level logs error events that might still allow the application to continue running.
6.	Fatal	Setting this level logs very severe error events that will presumably lead the application to abort.
7.	Off	Set this event level to turn-off file logging.

Logging Configuration

Log settings are configured differently for Self-Service, Password Center and the rest of modules. For the Self-Service and Password Center modules, GroupID provides logging configuration options for each Portal separately. For the rest of modules, GroupID provides a common tab on the **Configuration** dialog box from where you can choose the required logging levels for tracking events.

Configuring log settings for the Self-Service Portal

1. In the tree view of GroupID Management Console, expand the **Self-Service** node.
2. Next; under the **Portals** node, expand the required Portal and then click the **Servers** node.
3. Click the **Support** tab.
4. From the **Windows Logging** list, select the required level that you want to set for the Windows logging. Windows logging is explained earlier in this topic.
5. From the **File Logging** list, select the required level that you want to set for the file logging. File logging is explained earlier in this topic.
6. On the toolbar, click **Save** .

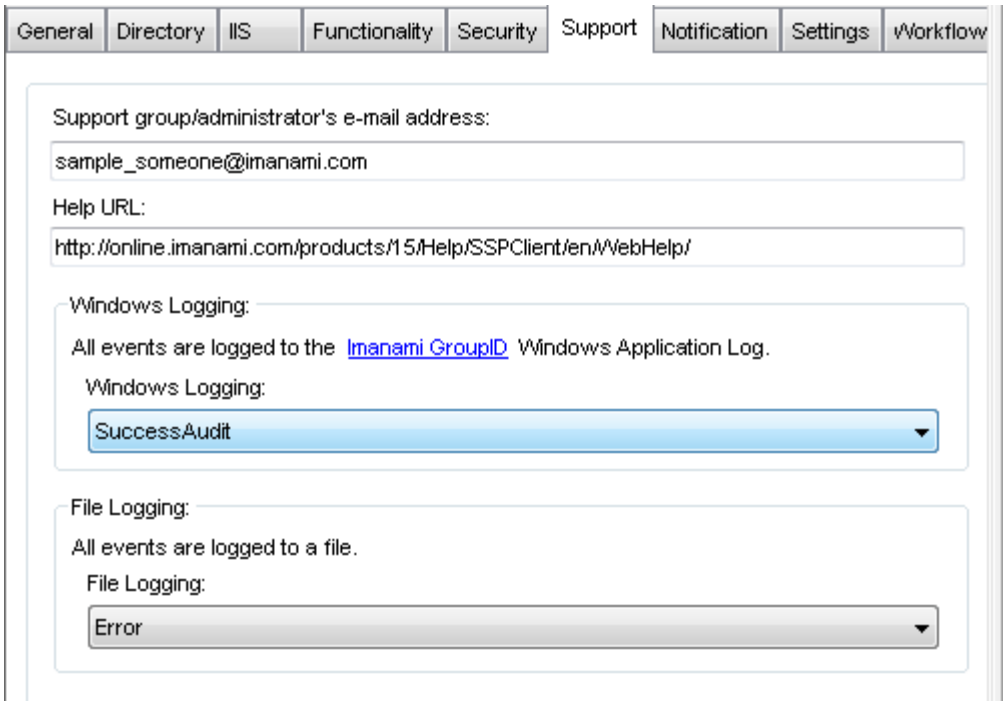


Figure - The Support tab

Configuring log settings for the Password Center Portal

1. In the tree view of GroupID Management Console, expand the **Password Center** node.
2. Next; under the **Portals** node, click the required Portal.
3. Click the **Support** tab.
4. Select the required logging level from the **Windows Logging** and **File Logging** lists.
5. On the toolbar, click **Save** .

Configuring log settings for Synchronize, Automate and Reports

- In the tree view of GroupID Management Console, click **Configuration** and then click **Modify System Configurations**. This displays the **Configurations** dialog box. On the dialog box:
    i. Expand the **Client** node, and then click **Log Settings**.
    ii. From the **Windows Logging** list, select the required level that you want to set for the Windows logging. Windows logging is explained earlier in this topic.
    iii. From the **File Logging** list, select the required level that you want to set for the file logging. File logging is explained earlier in this topic.
    iv. Click **OK**.

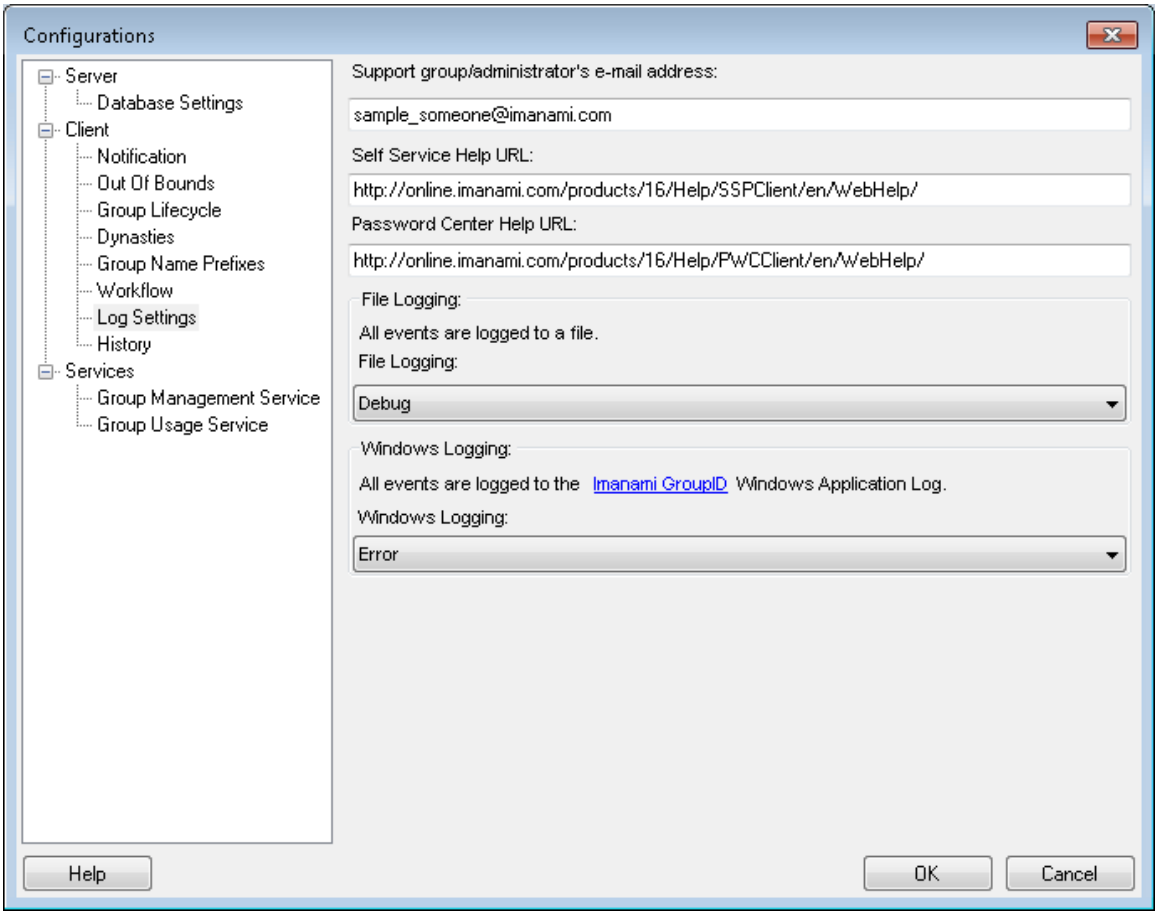


Figure - Log Settings

Notifications Settings

GroupID modules generate e-mail notifications on the occurrence of certain events; for example, expiry of groups, execution of a job, generation of workflow requests and similar. These notifications are sent to administrators, object owners or other specified recipients. Notifications require a SMTP server to be configured for sending e-mails.

Except for Synchronize, the notification settings for all GroupID modules are configured using the **Configurations** dialog box. Notification settings for Synchronize can be configured using the **Options** dialog box.

To configure the server:

1. In the tree view of GroupID Management Console, click **Configuration**, and then:

    - For Synchronize, click **Modify User Options** and on the **Options** dialog box, click **Notifications** under the **Synchronize** node.

    - For rest of the modules, click **Modify System Configurations** and on the **Configurations** dialog box, click **Notification** under the **Client** node.

In the **SMTP Server** box, type the fully qualified domain name or IP address of SMTP server. Outgoing and incoming e-mails will route through this server.

In the **From e-mail address** box, type the e-mail address to use for sending messages.

Click **Test** to check the server settings. GroupID will send a test message to the e-mail address specified in the **From** box using that e-mail address itself as the sender.

Click **OK**.

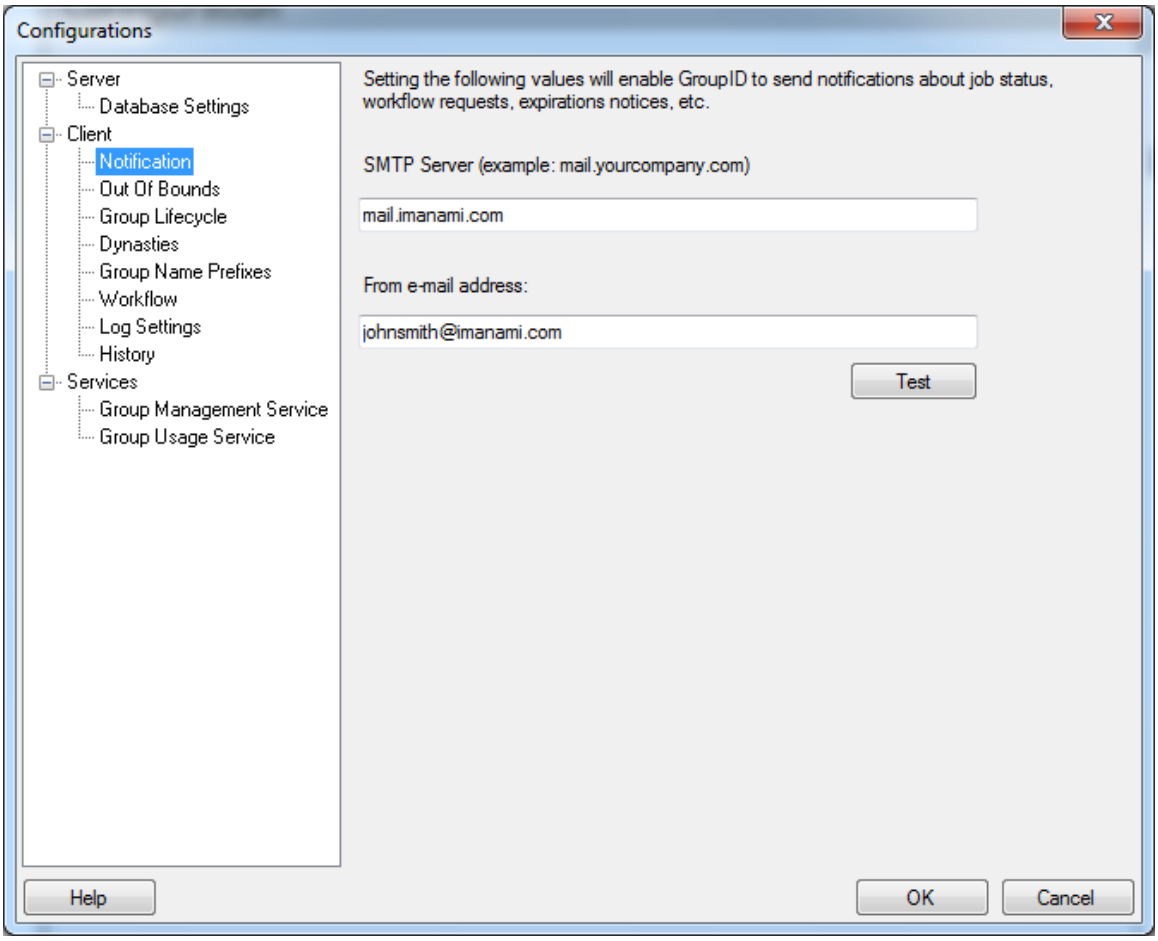


Figure - The Notification settings available on the Configuration dialog box

Group Name Prefixes

GroupID enables you to enforce naming consistency for groups by adding a prefix with their names and display names. These prefixes are defined globally and then used by Self-Service and Automate for assigning to the groups names. Once defined, GroupID makes it mandatory to select a prefix whenever a new group is created. For existing groups, adding prefix option is only available for unmanaged groups where you can optionally add prefix with the group name by simply modifying its properties; but once added, you cannot remove it. For managed groups, prefixes can only be added at the time of group creation and cannot be changed or removed later.

To add a new prefix that will be used by groups to add with their names, please follow the instructions below:

1. Click the **Configuration** node, and then click **Modify System Configuration**.
2. Next, expand **Client**, and then click **Group Name Prefixes**.

3. In the **Prefixes** area, click **Add**.
4. On the **GroupID** dialog box:
    i. In the **Group Name Prefix** box, type the prefix you want to add.
    ii. Click **OK** to close the dialog box.

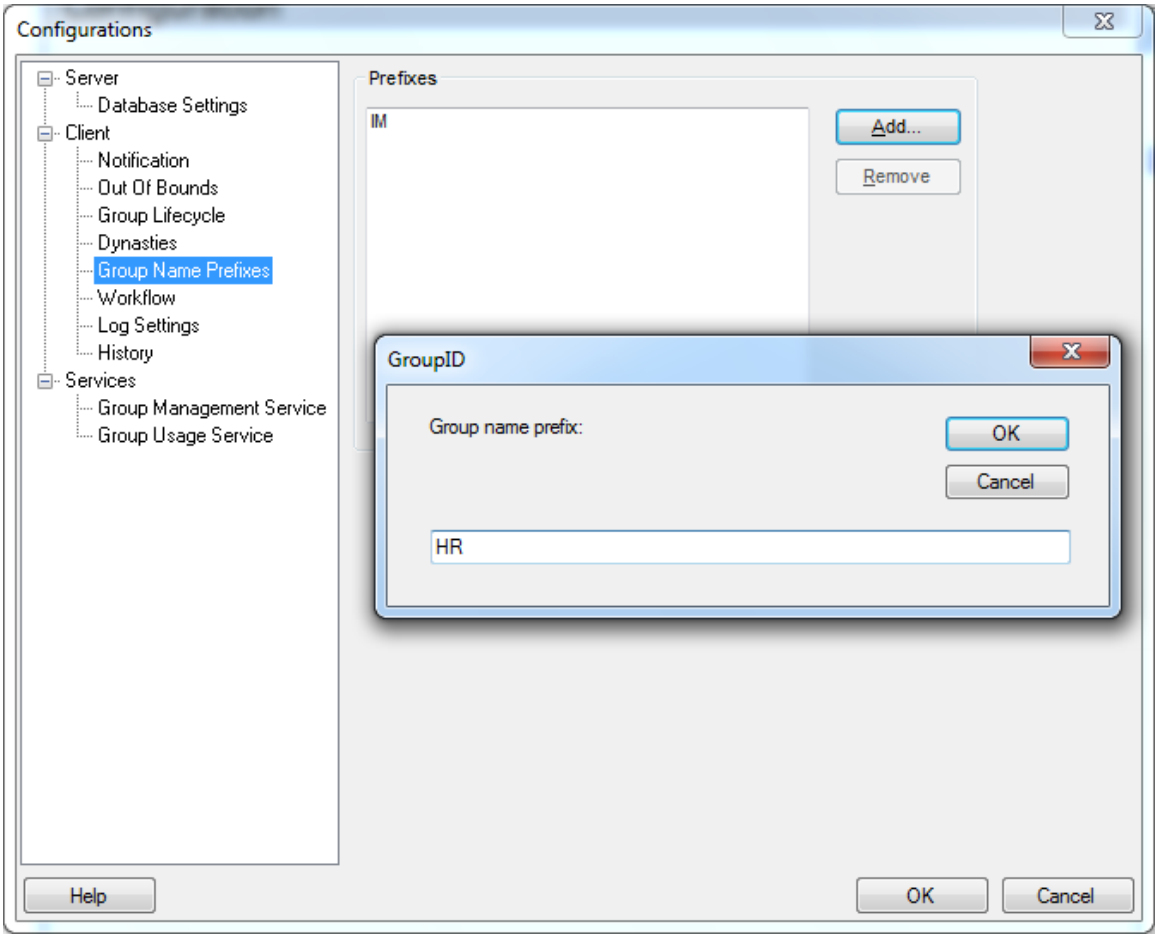


Figure - Imanami GroupID dialog box that opens up when Add button is clicked.

Database and the Data Service Settings

With GroupID 6, SQL Server is a requirement for running GroupID since many of its features depend on it for their working. History Tracking, Security Group Expiration and the Password Manager are some of the new features that depend on SQL Server. Along with this, to make GroupID more scalable and configurable, an alternate to extension attributes was necessary. Due to the limited storage capacity of extension attributes, supporting many of the advance features required in growing organizational setups would not have been possible.

GroupID supports all editions of Microsoft SQL Server 2005 and higher. If you do not already have or own an SQL Server, you can download the free Express edition from Microsoft's Web site.

To communicate with the SQL Server database, GroupID makes use of GroupID Data Service. This component is a part of the GroupID Setup and can be installed using the complete, or custom setup types on a computer running IIS. (To learn more about installing and setting up GroupID, please see the Installation Guide.) Like the database, GroupID Data Service can be installed on any computer in an environment that is running IIS and other GroupID clients can connect to it using a URL. A typical example of a data service URL is: **http://*machine name*/GroupIDDataService**.

Creating a new database

Great care needs to be put in to ensure that no more than one instance of GroupID database is running in your environment and that all GroupID clients are using the same database. Since GroupID stores all configurations and data for directory objects in its database, running and having clients connected to different instances of the database can cause unexpected results.

Before creating a new database, please confirm that one does not already exist. You only need to create a new database if GroupID 6 is new to your environment.

1. Click the **Configuration** node, and then click **Modify System Configuration**.
2. On the **Configurations** dialog box, expand **Server**, and then click **Database Settings**.
3. In the **Server name** box, enter the SQL Server name.
4. From the **Authentication** list, select any of the following according to your requirement:
    - **Use Windows Authentication** - Selecting this mode allows you to connect using your Windows user account.

      Please refer to Appendix E in GroupID Installation Guide to see if you can use this mode for connectivity.

    - **Use SQL Server Authentication** - Selecting this mode allows you to connect using your SQL Server user account.
5. In the **SQL Database**, type a unique name for the new SQL Server database.
6. Click **Create Database** to create the database with the entered name.
7. Click **OK**.
8. If the **Credentials** dialog box appears, enter the credentials for a user account having write permissions on the GroupID Data Service folder in IIS. The user name must be specified in the following format: ***domain name\user name*** (for example, acme.com\jsmith).

The database settings will be passed to GroupID Data Service where they are saved and are not stored locally on the computer.

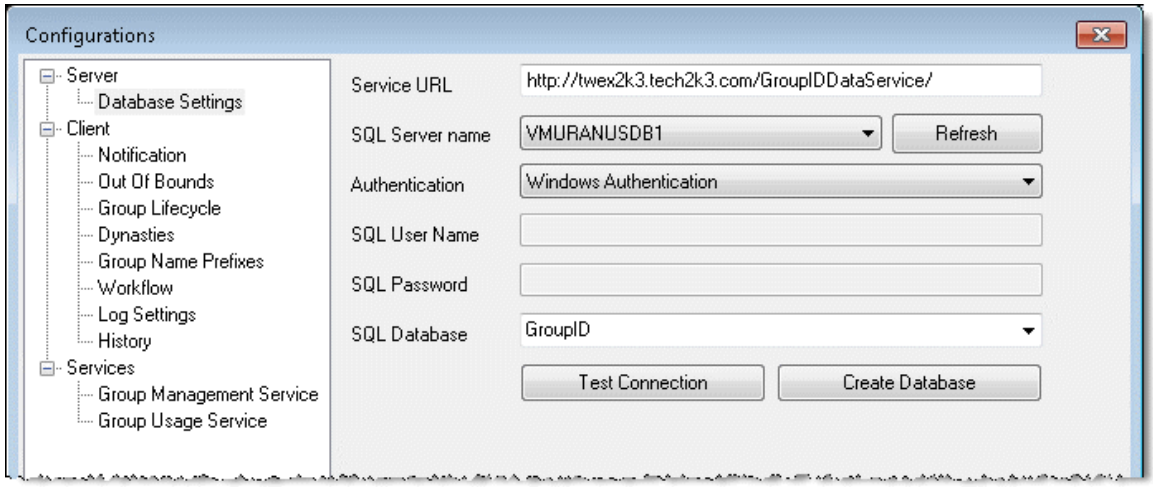


Figure - The database settings

Connecting to an existing database

You can connect to an existing database either using the Data Service URL or by providing the connection settings for SQL Server. The recommended practice is that once you have configured your database settings for the first time, you should use the GroupID Data Service URL to configure GroupID clients on other computers in your domain. You can set the data service URL using the following instructions:

1. Click the **Configuration** node, and then click **Modify System Configuration**.
2. On the **Configurations** dialog box, expand **Server**, and then click **Database Settings**.
3. In the **Service URL** box, enter the data service URL.
4. Click **OK**.

Once set, GroupID Management Console will retrieve the database settings from the service and display them.

History Settings

The history settings let you select the GroupID actions that you want to track and keep history for. Below is the list of actions GroupID can maintain history for:

Action	Description
Additional Owner Change	Tracks changes in additional owners.
Enrollment	Tracks members joining and leaving a group.
Expiration Policy Change	Tracks any changes to the expiration policy of a group.
Group Expire / Renew	Tracks group expiration and renewal actions.

Action	Description
OOB Change	Tracks out-of-bound change actions.
Ownership Change	Tracks changes to the primary membership of a group.
Query Change	Tracks changes to the query of a SmartGroup or Dynasty.
Security Type Change	Tracks changes to the security type of a group.
Workflow Approval / Denial	Tracks approval and denial actions for workflow requests.
All Others	Tracks all GroupID actions other then those mentioned above.

You can track all actions, only specific ones or can even disable this feature. History tracking feature has an impact on GroupID's performance. For optimal performance, Imanami recommends using this feature to track specific actions of importance only.

To configure history tracking, please follow the instructions below:

1. Click the **Configuration** node, and then click **Modify System Configuration**.
2. Next, expand **Client**, and then click **History**.

To track all actions

- From the **Track** list, select **All Actions**.

To track particular actions

- From the **Track** list, select **Selected Actions**.
- In the **Available Actions** list, select the actions that you want to track and move them to the **Selected Actions** list.
- Click **OK**.

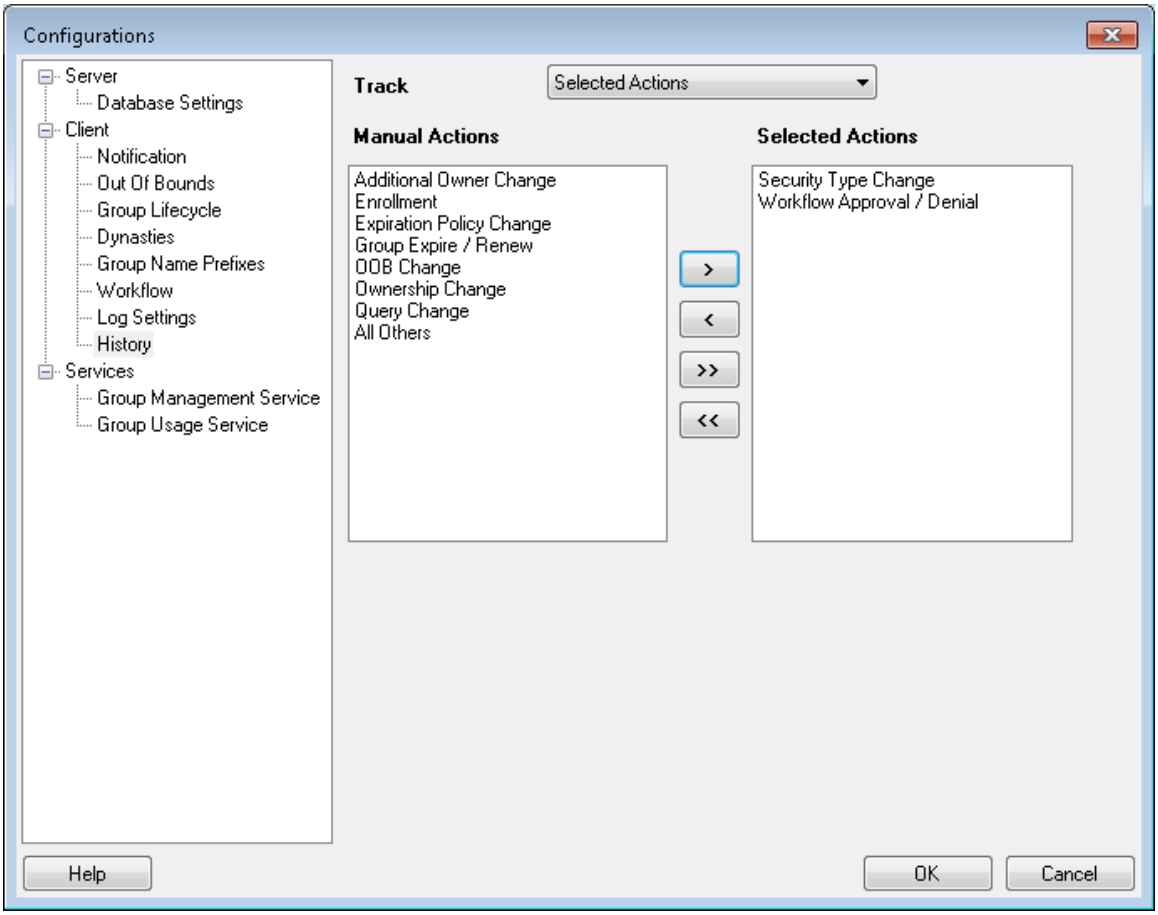


Figure - The History appearance for tracking Selected Actions only

To disable history tracking

- From the **Track** list, select **Nothing**.

Exchange Version Setting

GroupID uses Exchange schema attributes for creating mail-enabled AD objects, namely Groups, Users and Contacts. In networks that are running multiple versions of Microsoft Exchange, GroupID will use the highest version available as per its default behavior. Using the Configured Exchange setting, you can select and set a particular version of Exchange that you want to be used by GroupID. You can also restrict the creation of mail-enabled objects by setting GroupID to run in Active Directory (AD) only mode.

To configure the Exchange version:

1. Click the **Configuration** node, and then click **Modify System Configuration**.
2. Next, click the **Exchange** tab.
3. From the **Configured Exchange** list, select the Exchange version that you want to set. If you want to restrict the creation of mail-enabled objects, select **ADOnly** from the list.
4. Click **OK**.

Index

A

Active Directory, vii, viii, ix, 2, 3, 4, 5, 6, 10, 12, 13, 14, 18, 19, 23, 25, 27, 33, 34, 37, 42, 43, 46, 57, 58, 63, 69, 71, 72, 73, 74, 91, 92, 95, 96, 98, 103, 107, 109, 110, 111, 112, 114, 115, 132, 137, 139, 143, 147, 153, 159, 161, 162, 163, 170, 171, 178, 179, 184, 192, 195, 199, 202, 203, 204, 205, 206, 219, 222, 229, 241, 257, 262, 267, 269, 275, 282, 287, 293, 298, 303, 304, 306, 336
AD, 103, 336
Address Book, viii, 170, 175
Address Lists, viii, 170, 174
Alias, 123, 128, 182, 188, 190, 191, 317
Approver, 58, 60, 64, 65, 66, 67, 68, 143, 144, 149, 150
Assembly References, ix, 246, 261
Automate, viii, 3, 5, 6, 9, 11, 18, 105, 106, 107, 108, 109, 110, 111, 113, 115, 116, 119, 120, 126, 132, 134, 138, 139, 140, 142, 144, 145, 147, 148, 150, 152, 159, 161, 167, 168, 178, 179, 188, 189, 190, 192, 193, 200, 206, 295, 326, 328, 331
Automation, 3

B

Bad Words, viii, 69, 102, 103
Build Criteria, x, 274, 275, 282, 283, 285, 286

C

Container, 13, 20, 52, 53, 113, 121, 126, 129, 134, 137, 139, 140, 163, 180, 185, 220, 247, 277
Customize
  My Properties, viii, 69, 96
  Search Form, viii, 69, 91
  Update Wizard, viii, 69, 93, 97

D

Data source, 3, 5, 159, 161, 162, 163, 179, 184, 186, 195, 204, 205, 206, 211, 216, 218, 219, 230, 247, 251
Deletion, vii, viii, 16, 20, 119, 140, 141, 147, 148, 150, 151, 152, 155, 156, 255, 286
Delimiter, ix, 222, 263, 265
Deny, 57, 64, 66, 67
Distribution list, 18, 107, 109, 178, 201, 269, 270
DNS, 35, 43, 49, 309
Domain, vii, 2, 12, 13, 14, 15, 19, 20, 25, 27, 31, 33, 35, 37, 42, 43, 46, 53, 55, 75, 108, 111, 112, 113, 114, 115, 121, 125, 134, 139, 156, 165, 170, 171, 199, 200, 269, 272, 273, 283, 287, 293, 298, 306, 330, 333, 334
Domain Controller, 2, 25, 27, 33, 35, 43, 113, 114, 125, 170, 171, 199, 269, 272, 273
DTM, ix, 3, 246, 247, 248, 249, 251, 252, 253, 254, 255, 256
Dynasty, viii, ix, 105, 109, 121, 134, 144, 147, 177, 178, 179, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 335
Dynasty Options
  Geographical, 179, 183, 185, 190
  Managerial, 179, 183, 185, 186, 190
  Organizational, 113, 179, 183, 185, 190

E

Empower, 4, 33
Exchange, vii, viii, x, 2, 3, 10, 12, 13, 14, 19, 25, 34, 39, 63, 64, 105, 110, 115, 123, 128, 141, 142, 143, 170, 171, 172, 174, 175, 176, 178, 182, 186, 195, 198, 199, 202, 205, 267, 269, 270, 271, 325, 336
Exclude, ix, 148, 149, 185, 195, 206, 207, 253
Expansion Server, viii, 170, 174
Expiration Policy, 60, 109, 143, 144, 145, 146, 147, 148, 178, 200, 270, 334
Expire, 3, 17, 23, 59, 110, 143, 144, 146, 149, 155, 156, 200, 334
Expired, 17, 20, 54, 108, 109, 119, 143, 146, 147, 148, 150, 151, 152, 270
Expiry, viii, 7, 119, 125, 126, 140, 141, 143, 144, 148, 149, 150, 155, 156, 195, 200, 270, 329
Expression, 75, 76, 88, 110

F

File Logging, 326, 327, 328, 329
Filter, 52, 54, 63, 108, 110, 111, 148, 172, 173, 184, 195, 201, 253, 277
Functionality Mode
  Enterprise, 28
  Groups, 30
  Phonebook, 30
  Update Wizard, 29

G

Global Address List, 143
Global Catalog, 55, 113, 277
Global Script Editor, ix, 6, 246, 250, 251, 254, 255, 258, 260

Group, vii, viii, x, 1, 3, 5, 6, 12, 13, 14, 16, 17, 18, 19, 20, 23, 26, 30, 31, 37, 38, 46, 47, 48, 51, 52, 53, 55, 58, 59, 60, 62, 64, 102, 103, 105, 107, 108, 109, 110, 112, 113, 115, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 132, 133, 134,뢱137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 165, 166, 167, 168, 170, 171, 172, 173, 174, 175, 176, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 192, 193, 195, 199, 200, 201, 202, 204, 206, 207, 214, 270, 271, 272, 293, 294, 296, 297, 313, 314, 316, 319, 320, 325, 331, 332, 334, 335
QBDL, 105
SmartGroup, viii, 18, 119, 125, 126, 128, 131, 132, 133, 167, 178, 179, 185, 187, 188, 195, 196, 197, 335
Unmanaged, 17, 18, 105, 115, 119, 121, 159, 331
Group Lifecycle Management, vii, 16, 17
Group Management Service, viii, 20, 119, 134, 143, 144, 148, 149, 150, 155, 156, 157, 270
Group Name Prefix, x, 121, 127, 180, 325, 331
Group Scope
Domain Local, 20
Global, 19
Universal, 19, 165
Group Types
Distribution Groups, 18, 19, 143, 165, 181, 193
Security Groups, 18, 19, 46, 47, 60, 109, 148, 165, 178, 181
Group-by, 178, 179, 183, 184, 185, 188, 189, 190

H

HelpDesk, 23, 37, 38, 46, 47, 293, 295, 296, 308, 313, 319

I

Identity Management, 3, 23
IIS, x, 25, 36, 42, 44, 45, 293, 312, 316, 317, 318, 319, 332, 333
Importing, 159, 161
Include, ix, 149, 195, 200, 206, 207, 277
Inheritance, 189, 191, 193

J

Job
Files, ix, 216, 233, 237, 239
History, ix, 263, 264
Preview, ix, 216, 229
Run, 227, 228, 232, 233, 235, 238
Run Chart, ix, 213, 263, 264
Syncrhonize, 209, 211, 216, 224, 225, 238, 257, 265

L

LDAP, 18, 52, 107, 109, 125, 195, 211, 225, 262, 277
License, 6, 7, 122, 127, 143, 151, 181, 269
Licensing, vii, 1, 7
Linked Combo Types, 83, 90

M

Mailbox store, 201
Mail-enabled, 53, 59, 60, 105, 123, 128, 171, 172, 174, 175, 176, 182, 198, 199, 270, 271, 325, 336
Management Console, 1, 2, 5, 6, 7, 9, 10, 14, 26, 27, 33, 39, 40, 43, 44, 46, 48, 49, 50, 66, 70, 75, 83, 89, 90, 91, 93, 96, 98, 102, 103, 108, 111, 116, 148, 151, 155, 156, 159, 167, 168, 171, 179, 192, 193, 213, 229, 269, 275, 283, 285, 286, 287, 294, 295, 298, 310, 327,뢱328, 330, 334
Membership, viii, 3, 6, 12, 18, 19, 60, 105, 108, 109, 119, 125, 130, 133, 134, 139, 156, 158, 159, 160, 161, 165, 166, 167, 168, 169, 170, 175, 178, 179, 184, 185, 187, 188, 189, 192, 195, 204, 206, 270, 271, 335
Microsoft Management Console, 9
Move, 139, 279
Moving, viii, 89, 119, 139
Multi-Valued, 71, 73, 155

N

Namespaces, ix, 246, 261, 262
Navigation Bar, viii, 56, 69, 98
Nesting, viii, 158, 165
Notification, vii, 18, 42, 49, 50, 52, 58, 61, 65, 67, 109, 125, 134, 137, 138, 143, 149, 155, 168, 200, 212, 223, 224, 289, 294, 295, 305, 308, 309, 310, 329, 330

O

ODBC, 204, 211
Organizational Unit, 113, 139, 148, 149, 185
Originator, 175
Output Formats, x, 267, 268, 273, 276, 278

P

Password Expiry, ix, 125, 126, 195, 200, 201
Portal, vii, x, 6, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 53, 55, 56, 58, 60, 61, 65, 69, 70, 71, 75, 83, 89, 90, 91, 93, 96, 98, 100, 102, 103, 155, 156, 291, 292, 293, 294, 295, 296, 297, 298, 301, 303, 306, 308, 309, 310, 312, 316, 318, 319, 320, 326, 327, 328

Q

Query Based Distribution Group, 105
Query Designer, ix, 105, 129, 184, 186, 195, 198, 200, 201, 202, 204, 205, 206, 207

R

Recipient, viii, 14, 113, 170, 175
Renew, 3, 17, 23, 147, 150, 334
Report Categories, x, 267, 268, 269
Reporting, 283, 284
Rollover Logging, 327

S

Schedule, 4, 18, 119, 130, 132, 133, 134, 135, 136, 137, 138, 187, 188, 192, 211, 216, 225, 227, 228, 235, 236, 237, 287, 288
Scheduling, viii, ix, x, 119, 133, 134, 135, 136, 138, 188, 211, 216, 235, 237, 274, 287, 288
Script Editor, ix, 220, 244, 246, 247, 248, 250, 256
Scripting, ix, 209, 211, 220, 244, 246, 250, 261
Security Type, vii, 16, 18, 122, 127, 181, 335
  Private, 3, 18, 108
  Public, 3, 18, 108, 109, 198
  Semi-Private, 3, 18
  Semi-Public, 3, 18
Self-Service, 5, vii, 4, 5, 6, 10, 11, 18, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 39, 40, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 56, 58, 60, 61, 66, 67, 69, 70, 71, 72, 74, 75, 83, 89, 90, 91, 93, 96, 98, 102, 103, 122, 127, 143, 151, 155, 156, 181, 213, 318, 326, 327, 331
SharePoint, 24
SmartDL, 3
SmartGroup, viii, 18, 105, 109, 119, 121, 125, 126, 128, 131, 132, 133, 134, 159, 167, 178, 179, 185, 187, 188, 195, 196, 197, 335
SmartR, 3
SMTP, 42, 49, 57, 58, 65, 143, 171, 308, 309, 325, 329, 330
Snap-in, 2, 9
SQL Server, 195, 204, 325, 332, 333, 334
Synchronize, ix, 4, 6, 10, 11, 209, 210, 211, 213, 216, 217, 220, 221, 222, 223, 224, 225, 229, 232, 233, 234, 235, 237, 238, 240, 246, 250, 254, 255, 256, 257, 260, 261, 262, 263, 264, 265, 326, 328, 329, 330

T

Transformation
  Join, ix, 240, 241
  Left, ix, 240, 243
  Script, ix, 240, 244, 248
  Static, ix, 240, 241
  Substring, ix, 242
Transformations, ix, 209, 211, 240, 250

W

WebDir, 3
Windows Logging, 326, 328, 329
Workflow, vii, 4, 21, 23, 26, 27, 28, 30, 49, 57, 58, 59, 60, 61, 62, 63, 65, 66, 67, 68, 329, 335

Management Concepts and Exchange **History and Exchange** Lifecycle Management Deletion Classifications Types Scope Configuration - Overview User Interfaces Settings Requests **Settings Configurations** a Request List attributes Settings - Overview Jobs Command-line Utility Groups Owners Expiry Settings History Management Service **Management Conceptss Classifications Jobs Jobs Jobs Deletion** Members Groups Settings **Memberships** Settings tabs from Address Lists Membership from Address Book to Send Out-of-Office Message for Non-Delivery Reports - Overview Options Settings**s Jobs** Options - Overview Command-line Utility Jobs **Options** Environments Object Restrictions by Synchronize View for Report Reports **for Report for Report** Settings **Settings Settings** Settings Name Prefixes Version Setting